mobile mentor

# GETTING STARTED WITH ZERO TRUST

## A Deployment Guide with Microsoft 365 E3 Licenses

www.mobile-mentor.com

mobile mentor

## ZERO TRUST MEANS

01 Modern security framework for the post-pandemic hybrid workforce.

02 Enhanced security across all devices and applications, include BYO.

03 Friction-less employee experience regardless of location.

**Zero Trust is not another software product you have to buy. It is a methodology, and a modern approach to security in this complex world of hybrid work and BYO technology.**

**This paper outlines how a zero trust architecture can be deployed using Microsoft 365 E3 / A3 / G3 licenses.**

**We also define the point where enterprises may want to consider the upgrade to Microsoft 365 E5/ A5 / G5.**

Denis O'Shea
Founder
Mobile Mentor

mobile mentor

# ZERO TRUST - OVERVIEW

Legacy security based on a network perimeter, or a castle-and-moat approach, is no longer fit for purpose. Companies are hiring and onboarding new employees remotely, often working on personal devices and using cloud applications, so the traditional network perimeter is long gone.

We used to be able to trust our VPN and our passwords. Now that trust has been broken and our VPNs and passwords are often the weakest link. We have entered an era of zero trust.

Zero Trust means "guilty until proven innocent." Every request to access company information is assumed to be a security breach. Each request gets explicitly verified and only the requested resource is provided.

If the request is indeed a breach, and the attacker gets a foothold in your environment, zero trust limits the blast radius by preventing lateral movement using least privileged access and just-in-time access.

## THREE PRINCIPLES OF ZERO TRUST

01

**VERIFY EXPLICITLY**
Check devices and identity on every access request.

02

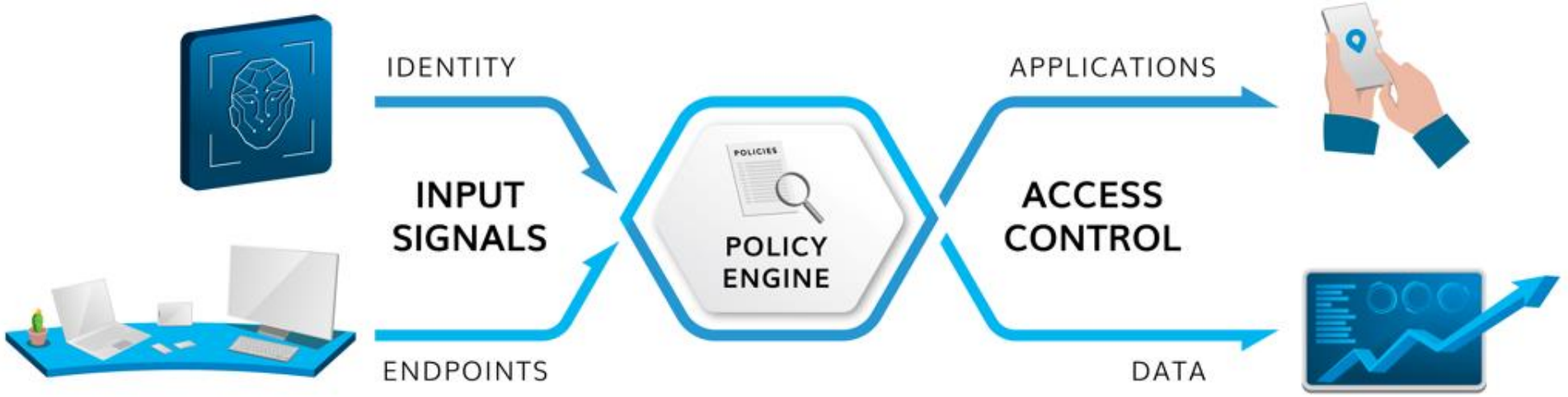
**ASSUME BREACH**
Assume every access request is a potential breach of your network.

03

**LEAST PRIVILEGE ACCESS**
Limit user access to only the requested resource.

mobile mentor

# INPUT SIGNALS – POLICY ENGINE – ACCESS CONTROLS




## SO HOW DOES ZERO TRUST WORK?

1 Gather signals from the person and device

2 Evaluate the signals in a policy engine

3 Grant access to only the requested resource

mobile mentor

# DEPLOYMENT BLUEPRINT WITH MICROSOFT 365 E3

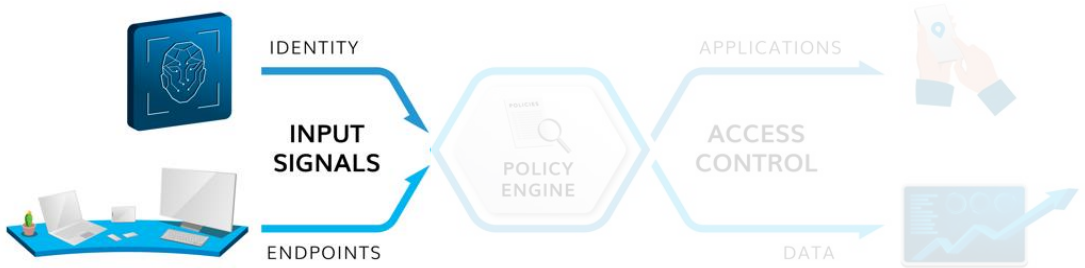
Zero Trust can be deployed effectively and at scale using standard Microsoft 365 E3 licenses.

The following section outlines practical guidance for the 3 parts of the Zero Trust architecture:

1. Input Signals
2. Policy Engine
3. Access Control

mobile mentor

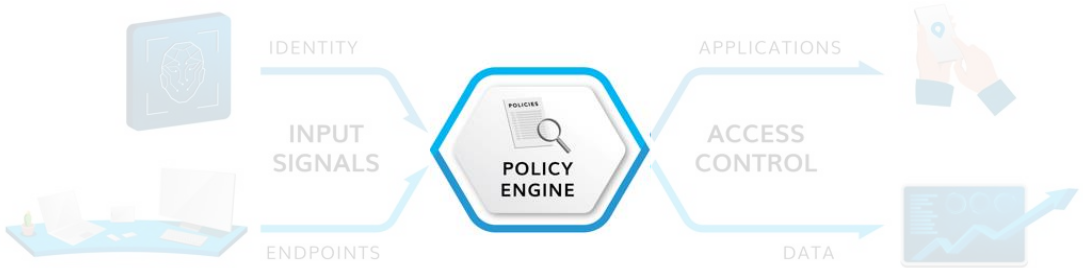
# GATHER YOUR INPUT SIGNALS




| Building Blocks | Cloud Identity | Corporate Devices | Personal Devices | Endpoint Protection | Device Encryption |
|---|---|---|---|---|---|
| Practical Guidance | Configure modern cloud identity with Azure Active Directory, biometrics, self-service password reset, multi-factor authentication, and single sign-on, if possible.<br><br>Decommission on-premise AD when possible and retire any tools that complicate your identity infrastructure. | Enroll all company owned devices, including laptops and smartphones, in Microsoft Endpoint Manager / Intune.<br><br>Legacy devices in SCCM can be co-managed in Intune, or Hybrid Azure AD Joined (HAADJ).<br><br>Ultimately you will want to migrate to Azure AD joined, and fully managed in Intune. | Protect Office 365 data on BYO and unmanaged smartphones via Intune App Protection Policies.<br><br>Assure your employees that their personal privacy is respected while company data is protected.<br><br>Use Azure Virtual Desktop or Windows 365 for BYO MacBooks, and Windows. | Configure Defender for Endpoints with anti-malware, web filtering and endpoint firewall to identify and block endpoint breaches.<br><br>Set-up rules to force the device back into a trustworthy state when it is compromised. | Avoid regulatory notifications for minor security incidents and reduce your insurance premiums by insisting on encryption for all devices.<br><br>This may require replacing old Windows devices that don't have a TPM 2 chip. |

mobile mentor

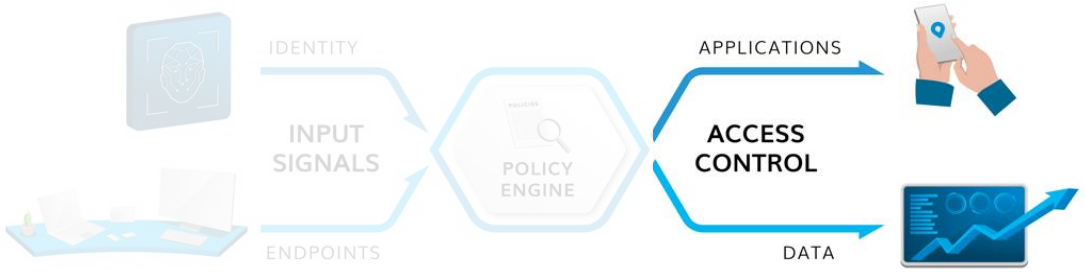
# BUILD YOUR POLICY ENGINE




| Building Blocks | Conditional Access | Change Management | Education |
|---|---|---|---|
| Practical Guidance | Configure risk-based Conditional Access policies in 'report mode' initially.<br><br>Then apply a gentle set of restrictions to high-risk situations and gradually tighten the policies as confidence and experience allows. | Employee push-back is inevitable as policies restrict certain activities that were previously permitted.<br><br>Ultimately the user experience will be much better, but it will be different and that requires a change management approach.<br><br>Regular communication to execs and end-users is critical to ensure the success of the Zero Trust journey. | Ensure your people are not the weakest link by providing a steady stream of security awareness education and communications on good security practices. |

mobile mentor

# ACCESS CONTROL




| Building Blocks | Risk Mitigation | Azure App Proxy & Private Link | Information Protection |
|---|---|---|---|
| Practical Guidance | Configure Defender for Office 365 to protect against malicious links, phishing attacks, attachments, and websites.<br><br>Configure Defender for Identity to limit lateral movement and account compromises in the event of a breach. | Eliminate the need for a VPN by using a secure connection to legacy applications and on-premise web apps with the Azure AD App Proxy.<br><br>For companies with substantial on-premise infrastructure, enable Azure Private Link to extend Zero Trust capabilities from the cloud to on-premise.<br><br>Azure Private Link can be skipped by going all-in with modern cloud applications. | Implement Information Protection by defining sensitive data categories and manually applying labels.<br><br>Assign policies to labels to trigger protective actions, such as encryption or limiting access to third party apps. |

mobile mentor

# BETTER SECURITY AND BETTER EMPLOYEE EXPERIENCE

The elegance of Zero Trust is that it improves endpoint security AND employee experience. This is very different to traditional security models where more security meant more restrictions.

Proactive IT leaders now have an opportunity to measure specific metrics before and after the deployment of Zero Trust to demonstrate the improvements in security and experience.

This visibility is important to stakeholders who invested in E3 and **want to see a return on investment** before committing to invest in E5 in the future.

## EMPLOYEE EXPERIENCE METRICS

- # OF DAYS TO ONBOARD NEW EMPLOYEES
- # OF MANUAL PROVISIONING REQUESTS
- # OF SUPPORT TICKETS AND CALLS
- # OF MANUAL LOGINS AND PASSWORD RESETS
- % OF APPS WITH SINGLE SIGN-ON

## ENDPOINT SECURITY METRICS

- # SECURITY INCIDENTS
- % FALSE POSITIVES
- % OF ENDPOINTS MANAGED
- % OF STAFF WITH MFA
- APP PATCHING METRICS

mobile mentor

# WHY UPGRADE TO E5?

As you can see in the section above, you can go a long way towards deploying Zero Trust with E3. At some point however, you will want to upgrade to E5.

E5 comes with a higher price tag, but the uplift from E3 to E5 is a small price to pay compared to the $9 Million cost of an average cyber security breach.

Here are 5 technical reasons to justify the additional investment in E5 security enhancements.

In Part 3 of this Zero Trust series, we explain **how E5 enhances a Zero Trust architecture, at enterprise scale**.

## E5 SECURITY ENHANCEMENTS

| | |
|---|---|
| **DEFENDER FOR ENDPOINTS** | Detect, analyze, investigate and remediate threats that will inevitably compromise some of your devices. |
| **IDENTITY AND ACCESS MGNT** | Add risk-based conditional access, identity protection, and privileged identity management |
| **DEFENDER FOR CLOUD APPS** | Limit shadow IT with an app vetting process to approve or deny the addition of new apps in your environment. |
| **INFORMATION PROTECTION** | Automate the Microsoft Information Protection process to apply labels and policies to sensitive data. |
| **COMPLIANCE MANAGEMENT** | Rules based on automatic retention policies and records management for advanced audit. |

mobile mentor

## ABOUT MOBILE MENTOR

Mobile Mentor is a global leader in the endpoint ecosystem and Microsoft's 2021 Partner of the Year in our field.

Certified by Microsoft, Apple and Google, our engineers live and breathe endpoint security and work tirelessly with our client to balance endpoint security with an empowering employee experience.

# ARE YOU READY TO GET STARTED WITH ZERO TRUST?

www.mobile-mentor.com

**United States** +1 877 707 3848
**New Zealand** +64 9 888 0512
**Australia** +61 2 9575 4827