mobile mentor

ZERO TRUST – AT SCALE

Enhanced Security with Microsoft 365 E5

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.

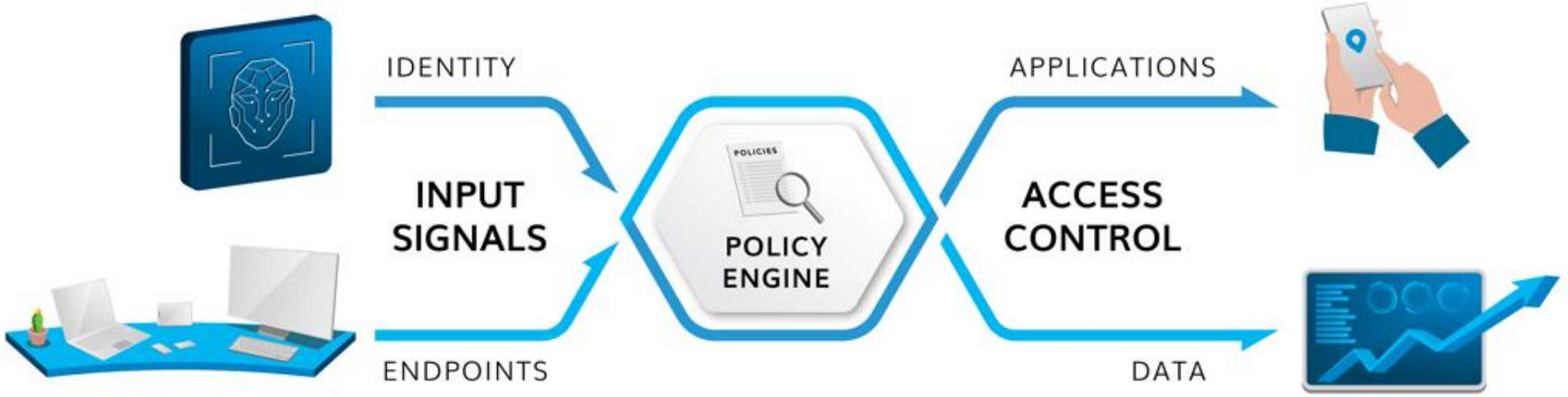
Zero Trust is not another software product you have to buy. It is a methodology, and a modern approach to security in this complex world of hybrid work and BYO technology.

This paper outlines how your Zero Trust architecture can be enhanced using Microsoft 365 E5 / A5 / G5 licenses.

Denis O'Shea
Founder
Mobile Mentor

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 the requested resource only

mobile mentor

ZERO TRUST ARCHITECTURE WITH MICROSOFT 365 E5

Zero Trust can be implemented with E3 but it can only be scaled effectively, with a high degree of automation, using E5.

This section outlines the main security enhancements to a Zero Trust architecture, at scale, using Microsoft 365 E5 licenses:

1. Defender for Endpoints
2. Identity and Access Management
3. Defender for Cloud Apps
4. Information Protection
5. Compliance Management

mobile mentor

DEFENDER FOR ENDPOINT

Defender for Endpoint P1 is included in the E3 license and provides a suite of tools to protect your devices including anti-malware, endpoint firewall, web filtering, controlled folder access and device control.

However, employees are fallible human beings so it is inevitable that some devices will get compromised.

When that happens, the ability to **detect, analyze, investigate and remediate** the threat is critical.

Defender for Endpoint P2 is included in the E5 license and provides the following additional capabilities:

1. Endpoint detection and response
2. Automated investigation and remediation
3. Threat and vulnerability management
4. Threat intelligence (Threat Analytics)
5. Sandbox (deep analysis)

mobile mentor

IDENTITY AND ACCESS MANAGEMENT

Azure AD Premium P1 is included in the E3 license and includes Conditional Access, multiple methods for MFA, the Authenticator app, Trusted IPs and Fraud Alert.

Azure AD Premium P2 is included in the **E5** license and provides the following additional capabilities:

1. Risk-based Conditional Access
2. Access Reviews
3. Identity Protection (risky sign-ins, risky users)
4. Entitlements Management
5. Privileged Identity Management (just-in-time access)

mobile mentor

DEFENDER FOR CLOUD APPS

Defender for Cloud Apps (formerly Microsoft Cloud App Security) is **ONLY available in E5**.

Most companies use far more cloud app than they realize. Many of these apps are **unapproved and not compliant with security policies**. Since employees are working remotely and accessing cloud apps from BYO devices, the risk of shadow IT is very real.

Defender for Cloud Apps provides the ability to:

1. Assess your app risk profile with a framework of 80 risk factors
2. Expose any compliance violations (HIPAA, GDPR etc)
3. Approve or deny the addition of new apps in your environment
4. Apply Conditional Access App Control (reverse proxy)
5. Protect sensitive data stored in cloud apps

mobile mentor

INFORMATION PROTECTION

E3 enables you to classify data and manually apply labels to sensitive data. You can then assign policies to those labels to trigger protective actions, such as encryption or limiting access to third party apps.

E5 enables you to fully automate this process with integration to Office 365 documents and data:

1. Protect sensitive information, regardless of where it is stored or who it is shared with (persistence).
2. Monitor, track and report on access to sensitive data and revoke access if needed.
3. Share data externally with partners and clients by defining permissions to view, edit, print or forward.
4. Manage your encryption keys with Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK).
5. For data outside Microsoft 365, use Azure Purview to automatically discover and map Azure data sources, on-premises, and SaaS data sources.

mobile mentor

COMPLIANCE MANAGEMENT

E3 enables you to manually apply retention labels and company-wide retention policies, and perform litigation hold so you can perform a basic audit.

E5 enables you automatically apply retention policies with the following capabilities for advanced audits:

1. Rules based automatic retention policies and records management with machine learning for retention.
2. Insider risk management, customer lockbox, privileged access management.
3. Advanced eDiscovery and advanced audit capabilities.
4. Address regulations and assess compliance with a risk-based score.
5. Third-party connections for external reporting.

mobile mentor

SUMMARY OF E5 ENHANCEMENTS

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.

To minimize the cost impact, here are 3 ideas:

1. Start with a small number of E5 licenses for the IT team to get visibility of shadow IT and threats
2. Consider E5 licenses for the highest risk users (e.g. the C-Suite) who receive the most phishing emails
3. Evaluate license needs for frontline workers to see if any users can be down-graded from E3 to F3

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 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.

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 ENHANCE ZERO TRUST?

www.mobile-mentor.com

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