EY IAM Zero Trust

Verify, then trust

Your digital world. Realized.

Building a better working world

Microsoft

Traditional perimeters are complex, increase risk, and are incompatible with today's business models

- With the modern workforce increasingly accessing applications from multiple devices outside the business perimeter, organizations risk being exposed to data breaches, malware and ransomware attacks.
- Today, information is spread across cloud, mobile and remote locations, making it more challenging to have a single security control for an entire network.
- Attackers are gaining access to the company networks and are free to move till they gain access to protected customer data, intellectual property or network controls, etc.
- Due to ongoing cyber-attacks, businesses are struggling to effectively manage and govern identities across business-to-employee (B2E), B2B and B2C environments.
- This affects brand trust and impact, leading to financial losses in terms of fines paid to regulators and restrictions on the ability to grow organically and inorganically.

Benefits of EY Identity Access Management (IAM) Zero Trust

- **Risk reduction:** Improve overall security posture by achieving lower breach potential and increasing secure network coverage
- **Audit and compliance:** Satisfy completeness and accuracy controls related to audits and consistently enforce policy-based controls and compliance initiatives
- **Organizational maturity:** Gain alignment and leverage synergies across multiple departments and improve maturity
- **Operational efficiency:** Automate manual processes and reduce the number of helpdesk calls
- **Business facilitation and end-user experience:** Transform EY IAM Zero Trust as an enabler for business, helping improve customer experience and thereby leading to increased growth
- **Overall visibility:** Gain visibility into users, devices and components across the entire network and get detailed logs, reports and alerts to detect and respond to threats
- **Fraud prevention:** Prevent customer fraud and strengthen protection against existing and evolving cyber threats
- **Cost avoidance:** Eliminate redundant tools and reduce infrastructure footprint by reducing business and organizational cybersecurity costs

Maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter

To protect themselves against the ongoing surge of cyber attacks, organizations need to move to a Zero Trust approach that operates more like a risk control framework. The EY IAM Zero Trust framework focuses on maturing key people, process and technology capabilities within your organization. It fits within the larger and holistic cyber program framework that defines the fundamental values of a risk-based, data-driven approach to security.

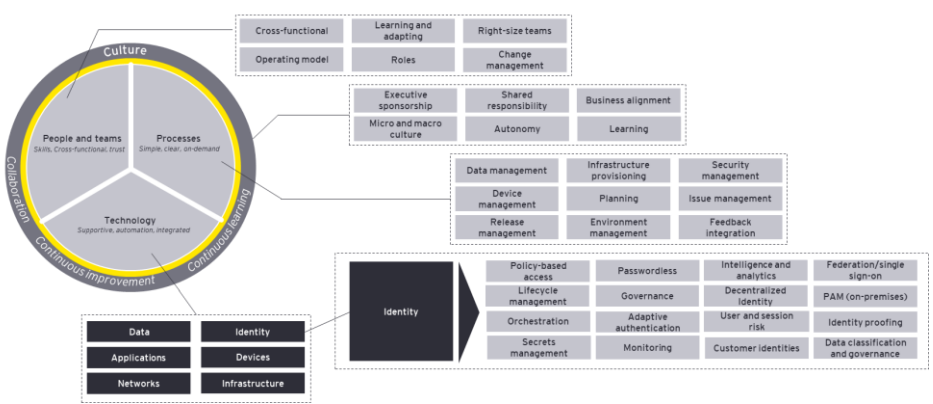
The EY IAM Zero Trust framework allows for cohesive Zero Trust architecture and recognizes that initial transformations require careful planning and strategy while later steps require deep technical knowledge. Adopting Zero Trust is a complex journey for clients that are used to the traditional model of IT security. The complete EY IAM Zero Trust transformation journey includes:

- Leveraging Microsoft Azure Active Directory P2 for addressing Zero Trust challenges
- Defining authorization strategies (consent, conditional access, policies) for maximizing security
- Implementing Microsoft Azure Key Vault as a secrets management solution

Key functionality

- Zero trust is not a technology but is a framework that includes technology and processes to secure five different types of assets: users, devices, data, network, analytics and automation.
- Zero Trust, in all its elements, overcomes modern security challenges by extending security beyond the perimeter and abiding by the principle of least privilege.
- The zero-trust policy enforcement dictates that no users or machines should be automatically trusted. The architecture will define how much of your Zero Trust Architecture (ZTA) is made up of software-defined perimeters, micro-segmentation, or governed by identity.

EY IAM Zero Trust framework



Source: Microsoft IAM Solutions Offering

Customer success stories: EY IAM Zero Trust in action

The client is one of the largest and fastest-growing employee-owned supermarket chains in the American retail sector. EY leveraged a team from multiple cybersecurity sub-competencies to execute the following engagement activities:

- Refer to EY frameworks for cloud security and IAM, along with industry-leading practices to document, analyze and assess potential gaps within the current Azure AD environment
- Leverage Microsoft 365 Secure Score to review security control configuration and analyze results against EY and cloud-integrated storage (CIS) security control standards to provide improvement opportunities
- Leverage MCAS portal to review alerts, policies, configurations and analyze results against Microsoft recommendations and EY Experience and frameworks

Client challenges

The client teams wanted assistance to:

- Assess their existing Microsoft Cloud App Security (MCAS), Microsoft Defender for Endpoint (MDE) and Microsoft Azure Active Directory (AD) capabilities and provide actionable recommendations
- Identify several initial areas of focus to prioritize efforts and develop a strategy and roadmap to elevate the security posture
- Expand their Microsoft Azure footprint and improve their posture on:
    - Cloud IAM and secure single sign-on (SSO)
    - Threat protection
    - Cloud application security

Client benefits

- Evaluated people, process, and technology components of the current security program
- Identified and prioritized opportunities for rapid improvement and to help drive the strategic priorities to expand Azure footprint
- Performed detailed AAD technical assessment through interviews and by running read-only PowerShell scripts
- Identified 13 high and medium priority observations and suggested recommendations
- Analyzed 17 configurations settings for alignment to best practices for threat detection and prevention
- Analyzed 42 configurations settings for alignment to best practices for cloud application and user behavior monitoring
- Recommended Zero-Trust adoption plan and phased MCAS roadmap for top identified cloud access security broker (CASB) use cases

EY and Microsoft

The digital technologies that are impacting your business today – social, mobile, analytics and cloud – are rapidly expanding to create new employee and customer experiences, fundamentally changing how your organization works, interacts and competes. The EY and Microsoft alliance combines EY deep insights and experience in disruptive industry trends, new business models and evolving processes with Microsoft scalable, enterprise cloud platform and digital technologies. EY and Microsoft can help accelerate digital transformation with advanced solutions that support enterprise strategy, transform customer and workforce experiences, create new, data-driven business models, build intelligent, automated operations and bring confidence that these innovative solutions are secure, compliant and trusted. Together, we can help accelerate digital strategy and amplify your business performance to thrive in a digital world.

For more information, visit: ey.com/microsoft.

Contact information

EY contacts:

Nicole J Koopman
Executive Director
Technology Consulting
Ernst & Young LLP United States
nicole.koopman@ey.com

Microsoft contacts:

Jodi Lustgarten
Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 006984-21Gbl

ED None

ey.com