EY Administration and Workplace Services Cloud Security Baseline Definition

Broad security monitoring solution for industries

Cloud misconfigurations are leading to costly data breaches

- COVID-19 pandemic has pushed businesses to move to a work-from-home model practically overnight, altering the enterprise landscape for 2021 and beyond. Companies in various stages of cloud adoption are struggling with defining and enforcing security and compliance requirements for cloud services deployed across cloud environments.
- Organizations that were already struggling to manage and secure their physical IT infrastructures that had expanded with mobile and IoT devices now have to face additional challenges. As a part of the cloud transformation journey, they have to identify and define security baselines and requirements for deploying secure and compliant resources.
- According to a study conducted by Gartner in 2019, "by 2025, 90% of the organizations that fail to control their public cloud use will inappropriately share sensitive data" as experts believe this could lead to leakage and compromise of sensitive corporate data. Moreover, moving to the cloud has further intensified an already obscure and problematic task–visibility and control of what connects to the corporate network.
- According to the 2020 Trustwave Data Security Index report, 96% of organizations across the globe plan to transfer sensitive data to the cloud within the next two years. Therefore, the chief information officers (CIOs) have to deal with the enormous task of developing a robust enterprise strategy even before implementing the cloud or risk the aftermath of an uncontrolled public cloud as breaches could get even uglier in an insecure cloud environment.

Benefits of EY Administration and Workplace Services Cloud Service Security Baseline Definition solution

- Safeguard cloud infrastructure to protect organizations from data breaches by defining secure configuration baselines
- Help enforce compliance for specific resource configurations and improve the business's cloud security posture by mapping baselines to control frameworks
- Increase deployment speed to reduce the likelihood of potential misconfigurations and vulnerabilities in your cloud environment
- Decrease support time associated with remediating misconfigured resources
- Proactively update Infrastructure-as-Code (IaC) with defined security baselines to help developers deploy secure resources without an unintentional compromise on security
- Integrate defined baselines with Microsoft-native capabilities for detecting non-compliant resources for cost reduction, ease-of-use and improved integration with the overall Microsoft ecosystem
- Eliminate alert fatigue and human error associated with the manual identification, prioritization, and remediation of cloud misconfiguration

EY Administration and Workplace Services Cloud Service Security Baseline Definition solution provides secure configuration requirements for cloud resource deployments

EY teams are helping organizations to design and define cloud security baselines for Microsoft Azure services to help organizations consistently deploy cloud resources in compliance with organizational and regulatory compliance requirements to operate securely in the cloud. Our full range of security capabilities helps clients secure cloud environments in a more proactive, preventative approach versus a reactive, manual approach to enforcing compliant cloud environments.

The EY Administration and Workplace Services Cloud Service Security Baseline Definition solution is part of the EY Cloud Security product suite, built on the EY Cloud Security Framework. The security baseline definition service is architected to utilize Microsoft-native security capabilities built within the Microsoft family of services.

Target audience:

- Chief Information Security Officer (CISO)
- Chief information officer (CIO), technology principal
- Chief transformation officer (CTO)
- Cloud security director
- Information security director
- Business owners

Target industries:

- Advanced manufacturing and mobility
- Agriculture
- Life sciences
- Consumer products and retail
- Financial services
- Oil and gas
- Power and utilities
- Energy
- Chemicals
- Media and entertainment

Key functionality

EY Administration and Workplace Services Cloud Service Security Baseline Definition solution helps consumers define secure configurations mapped to frameworks to build and deliver secure compliant cloud environments.

Cloud security framework + Industry and regulatory frameworks

CCM GLBA NIST PCI FFIEC ISO ITIL COBIT

Azure Kubernetes Services	Azure DevOps Pipeline	Azure Container Registry

• Define network policy for clusters
• Set security policies to pods in Azure Kubernetes Services
• Restrict pod privileges
• Define Azure Active Directory service principles
• Define and use pod managed identities
• Use Azure Key Vault provider with secrets store
• Use Container Storage Interface (CSI) Driver for managing pod secrets
• Integrate Azure Active Directory in Azure Kubernetes Services
• Define Role-Based Access Control (RBAC) Azure Key Vault (AKV) policies
• Restrict application programming interface (API) server access
• Define metadata access restrictions
• Audit logging
	• Set the release retention policies for a release pipeline to define for how long a release and the run linked to it are retained before being deleted
	• Set the appropriate permissions and security role for pipeline for the following components:
	  • Pipelines
	  • Releases
	  • Task groups
	  • Deployment pools
	  • Service connections
	  • Library artifacts
		• Protect resources using Network Security Groups or Azure Firewall on the Virtual Network
		• Enable DDoS standard protection on the virtual networks
		• Use single sign-on (SSO) with Azure Active Directory
		• Use multi-factor authentication for all Azure Active Directory-based access
		• Enable audit logging for Azure resources
		• Configure central security log management
		• Encrypt all sensitive information in transit
		• Encrypt sensitive information at rest

Baseline security standards definitions for all cloud services

- Security standards baselines created to support deployment of cloud services based on defined frameworks and requirements.
- Repeatable requirements based on defined baselines for secure architectural and engineering solutions.

Customer success stories: EY Administration and Workplace Services Cloud Service Security Baseline Definition solution in action

EY teams were engaged by a large American international life sciences company to mature their cloud security monitoring and response capabilities. The objective of the collaboration between the client and EY teams was to define cloud security service baselines within the Microsoft Azure environment for development teams to deploy secure and compliant resources.

Client challenges

- Lack of cloud security knowledge and skillsets within the current operating model
- No defined cloud security framework or requirements for deploying secure cloud environments
- Inability to detect and respond to misconfigurations within Microsoft Azure environments

Strategy

- Identified and documented cloud security baselines based on security frameworks and Microsoft Azure Security Center findings
- Identified Infrastructure-as-Code gaps for each supported service
- Facilitate logging and monitoring capabilities to detect misconfigurations

Results

- Documented Microsoft Azure service security baselines for approved services
- Improved Infrastructure-as-Code templates by providing recommended updates based on gap analysis, utilizing defined service standards
- Operationalized monitoring and response capabilities based on defined security baselines

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:

Alex Shulman
Executive Director
Cloud Cybersecurity Leader Americas
Consulting, Technology Consulting, Cyber Security
Ernst & Young LLP United States
alex.shulman@ey.com

Bhumi Bhuptani
Senior Manager
Consulting, Technology Consulting, Cyber Security
Ernst & Young LLP United States
bhumi.bhuptani@ey.com

Evan Thomas
Manager
Consulting, Technology Consulting, Cyber Security
Ernst & Young LLP United States
evan.thomas@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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

EYG no. 000149-22Gbl

ED None

ey.com