Tech Mahindra

Secure your Azure Cloud Journey with **Tech Mahindra**

Tech Mahindra's Security Assessment for Azure for a seamless & Secure cloud lifecycle management

Gold
Microsoft Partner
Azure Expert MSP
Microsoft

Partner Advanced Specialization
Kubernetes on Microsoft Azure

Tech Mahindra

68% Organizations have misconfiguration of cloud platform security policies / wrong setup

69% Organizations lack framework to secure data on cloud resulting in Data loss / leakage; Data privacy / confidentiality breach

To embark on your cloud journey and be successful you need a well-defined strategic roadmap. Tech Mahindra's Cloud security assessment aligned to Microsoft's cyber defense and zero trust framework for Azure provides a robust cloud strategy which takes a data-driven approach to deep dive into the current IT landscape, provide a comprehensive assessment and present a crystal-clear executable plan.

CHALLENGES

- Lack of cloud security preparedness due to legacy infrastructure & strategy direction
- 60% to 70% Cloud migration projects face deficiency of cloud security experts to extend support during assessment and planning stage
- Stitching together a holistic approach from network, endpoint, application and data security along with risk and compliance is a mammoth task
- Procuring resources with diverse skillset to define strategy and roadmap along the life cycle of cloud migration needs huge investment,

01

IDEAL SOLUTION

- Tech Mahindra's holistic Cloud security approach helps customers accelerate their enterprise cloud journey by getting it right in the first go with the right cloud strategy
- Our proprietary security assessment solution is developed for every stage of the enterprise cloud adoption journey while aligning them to portfolio of services to Microsoft's cyber defense and zero trust framework for Azure
- Covers the entire cloud adoption journey - Cloud Strategy Consulting; Accelerated Cloud Migration; Intelligent Cloud Operations/ Data and Analytics; Edge/Hybrid Computing and Enabling Cloud Native Applications, managed security and digital transformation

02

DESIRED OUTCOMES

- Faster time-to-market – **ready to use assessment templates reduces 2X migration timeline while** maintaining the secure state.
- **30% reduced costs -** Exhaustive, matured, automated, template-based assessment reducing delivery risks and assessment phase timelines by **3X**
- **30%** enhancement in security posture with expert recommendation
- **100%** coverage on security benchmarks and standards

03

TECH MAHINDRA SECURES ENTERPRISES AT EVERY STEP OF THE CLOUD JOURNEY

Tech Mahindra

ORGANISATION CLOUD JOURNEY

ROADWAY TO SUCCESSFUL CLOUD TRANSFORMATION

1. CLOUD STRATEGY & ROADMAP
2. DESIGN & PLANNING
3. CLOUD MIGRATION
4. CLOUD OPERATE
5. DIGITAL TRANSFORMATION

OFFERINGS

- Cloud Readiness Assessment
- Application Portfolio Optimization and security assessment

- Security policy Standardization
- Multi Cloud Adoption security assessment
- Security tools compatibility assessment
- Industry compliance and benchmarks assessment

- Priority migration assessment for security tools
- Assessment and roadmap on security models like zero trust and DiD
- Risk assessment and mitigation

- Cloud Governance & Operating Model
- Continuous compliance and risk monitoring and reporting
- Security posture assessment and enhancement
- Gap assessment of security policy and controls
- Assessment of compatibility and interoperability of existing security tools
- Assessment of compliance and standards
- Assessment of risk and mitigations

BUSINESS VALUE DELIVERED

- Reduced time in planning
- Reduction in investment on procuring resource with expertise on all security domains
- Enhance Planning and Execution

- Foundation for Cost Transformation Initiatives
- Redefining Cloud Operating Model

- Governance Structure
- Adoption of secure cloud models
- Optimized policies for risk and governance

- Building best practices
- Setting up deployment plans & cloud operating models

- Auditing and prioritizing scenarios
- Unified Security & Compliance Ecosystem
- Ready to use recommendations on compatibity and interoperability of new state
- Shorter time to security design for digital transformation

ACCELERATORS/ FRAMEWORKS

Passport NxT

MAC

Blue Marble
Tech Mahindra Business Services Integration Platform

mPAC™
Managed Platform for Adaptive Computing

NIST

CSA cloud security alliance®

ORGANISATION CLOUD TRANSFORMATION JOURNEY END STATE

Cloud Security Assessment Offerings

Pre Migration

- Pre Migration Security Landscape Assessment
- Application and security tools optimization
- Identification of cloud native and 3rd party tools
- Identification and mitigation of risks and gaps
- Report on existing security posture of applications and infrastructure

Migration

- Assessment of migration strategy with prioritization security tools and controls.
- Assessment of compatibility of security tools relative to each other and cloud environment
- New controls and compliance requirement for cloud environment

Digital Transformation

- Assessment of compatibility of existing security tools and controls
- With transformation and new integration
- Risk assessment and mitigation plan
- Assessment of compliance and security posture of new state.

Managed Security

- Periodic assessment of cloud security posture and recommendations on enhancement
- Continuous monitoring and reporting of compliance and application security
- Risk and threat monitoring and reporting

Future Roadmap – Zero Trust Assessment & implementation (Maturity Model)

TechM is focused towards continuous innovation and integrations with trending and emerging technologies and solutions in association with our valued partners like Microsoft. Here we present you a preview on the upcoming offering on Zero Trust security and it’s maturity stages.

	Traditional	Advanced	Optimal
Identities	On premise Identity provider No SSO between on prem apps and Cloud Restricted view of Identity Risk	Federation of Cloud Identity with On-Prem system Condition access policies for access and remediation Analytics for better visibility	Password less authentication User, device, location and behavior is analyzed in real time for risk assessment and security
Devices	Domain joined devices managed with Group policies Objects or Config Manager Devices need to be on network for data access	Device Registration with Cloud Identity Provider Access restricted to cloud managed and compliant devices DLP control for corporate device and BYOD	Endpoint threat detection to monitor device risk Access Control is gated on device risk for corporate device and BYOD
Apps	On-prem app access via physical Network or VPN Some critical cloud applications are accessible to users	Internet facing on-prem apps and cloud apps with SSO Cloud shadow IT risk assessment, monitoring and controls on critical apps	Least privilege access with continuous verification for all apps Dynamic control for all apps with in-session monitoring and response
Infrastructure	Permissions managed manually across environments Configuration management for VMs and servers on which workloads are running	Workload monitoring and alerting for abnormal behavior Workload assigned App Identity Just-in-time access control on resources for human access	Unauthorized deployments and blocked and alerted Granular visibility and access control are available for all workloads Segmentation for user and resource access for all workloads
Network	Flat open network with few network security Perimeters Minimal threat protection and static traffic filtering No encryption for internet traffic	Many ingress/egress cloud micro-perimeters with some micro-segmentation Cloud native filtering and protection for known threats	Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation ML-based threat protection and filtering with context based signals
Data	Access governed by perimeter control instead of data sensitivity Sensitivity labels are applied manually with consistent data classification	Data classification and labeling with regex/keyword methods Access decisions governed by encryption	Classification augmented by smart ML models Access decisions governed by cloud security policy engine DLP policy secure data sharing with encryption and tracking

Tech Mahindra

LEADING FIBER BASED PRODUCT MANUFACTURER

CLIENT

DELIVERING BUSINESS VALUES

BUSINESS CHALLENGES

- Global presence with emerging B2B and B2C capabilities but lack of comprehensive security framework
- High % of legacy technologies and tools not capable of defending present day threats
- Multi-cloud environment with regional security preferences
- Acquisitions and mergers lead to lack of uniform tools Imperative to Modernize / Transform the infrastructure & Security Services utilizing Cloud based services
- Users located at diverse locations and lack of user account monitoring and security for privilege accounts
- Need for a professionally managed service provider for end-to-end Cloud Security and Stabilization (Sec-Ops)

TECH MAHINDRA APPPROACH

Cloud Readiness Assessment to achieve:

- 6R assessment of infra patterns, COTS and in house apps for rationalization and security framework
- Did assessment of existing IT landscape and established cloud security model based on TechM security framework, Azure cyber security framework and NIST guidelines.
- Did gap and risk analysis for obsolete tools and provided recommendations based on zero trust and DiD for cloud native and 3rd party tools like Sentinel Azure DDOS, MCAS, CheckPoint IPS, Palo Alto FW
- Did assessment for IAM landscape, users and regions. Provided Azure native solution for MFA, SSO and ADFS

Future State Operating Model

- Post Assessment helped the customer to build strategy for digital transformation of infrastructure security from legacy tools to NextGen layer 3 to layer 7 tools
- After evaluation created a Security operations framework for cyber defense of multi cloud environment of customer with added defense to crown jewels
- Did assessment of the business boundaries and regional compliance requirements and helped customer build security and compliance policies
- Provided best practices and guidelines for security of endpoints with EDR capabilities

VALUE DELIVERED

- 40% Improvement in workload visibility and management with EDR and SIEM
- 60% improvement in application and data security with MCAS and WAF
- Improved and secure access solution with Azure ADFS and MFA
- 2x improvement in threat detection and response
- 40% improved security posture with modern cloud native security controls
- 70 % reduction in attack surface with Zero trust and azure cyber security framework

Tech Mahindra

LEADING LIFE INSURANCE AND ASSET MANAGEMENT COMPANY APAC

CLIENT

DELIVERING BUSINESS VALUES

BUSINESS CHALLENGES

- Complex IT landscape: Lack of strong IAM solution.
- High % of legacy technologies and security tools. Many were outdated
- Multi-cloud environment with regional security preferences
- Lack of application scanning and monitoring
- No standardization for security policies and monitoring
- High mix of service providing vendors and partners

TECH MAHINDRA APPPROACH

Cloud Readiness Assessment to achieve:

- 6R assessment of infra patterns, COTS and in house apps
- Did Assessment and established model and policies for IAM with forgerock and Azure AD
- Did assessment for endpoint security and established deployment plan for Defender and cyberreason
- Post gap analysis helped customer to improve security posture with CyberArk as PIM
- Did assessment for Security operations. Created roadmap for splunk extension to cloud workloads.

Future State Operating Model

- Tooling selection for cloud operations: governance and FinOps
- Post assessment helped customer to upgrade infrastructure defense from network firewall to application firewall
- Created future roadmap for Splunk to Sentinal transformation for SIEM and SOAR capabilities
- Post assessment provided best practice for O365 security
- Post assessment of benchmarks and compliance, provided recommendation on data encryption with Azure native key vault and Azure container security services.

VALUE DELIVERED

- 40% improved security posture
- 80% reduced time in security policy implementation
- Better visibility of workloads with continuous monitoring for compliance
- Robust framework for application security with WAF
- Improved security and access control
- Future ready defense with zero trust and DiD

Tech Mahindra

Tech Mahindra's Azure Cloud Services

Tech Mahindra's Azure Cloud Services

CALL FOR MORE INFORMATION:

+91-8951000900

REACH OUT TO US AT:

microsoftgtm@techmahindra.com

ASK A QUESTION VIA EMAIL:

microsoftgtm@techmahindra.com

LEARN MORE:

Tech Mahindra Cloud Security

Tech Mahindra Microsoft