

EPAM Azure Security Assessment

March 2024

Cloud – a New Security Paradigm

Tech Landscape Evolution

Technology around us is changing rapidly. The introduction of novel technologies is mostly driven by a huge push to automation and scalable deployment of services in the industry. Cloud is a new normal.

IT Threat Evolution

Cyber attacks are becoming increasingly complex and frequent, with machine-based algorithms expected to become the primary threat actors in the future, evolving quickly, based on the massive amount of usable data, and aiming at infrastructure and services complexity and granularity.

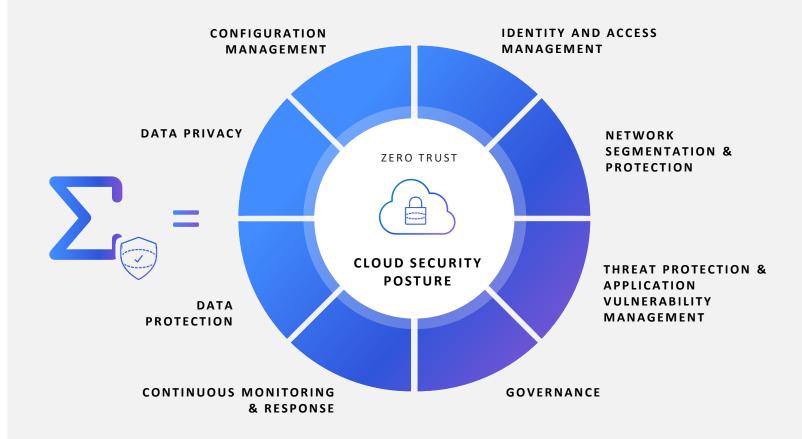
Analytical Usage Risks

Analytical data usage is growing. Analytical usage conflicts with the current security model applied on the operational systems. Data Analysts typically want to get access to all data and multiple data sets. Cloud is there to support this trend – but with this, a new risks paradigms emerge.

Our Approach to Cloud Security — Security by Design

Holistic approach to security and privacy in the cloud looks at the entire ecosystem of living controls from the conception to run-time.

Our Security by Design approach infuses security and privacy into Cloud DNA at every step of the way and in line with all the applicable regulatory requirements.





Our Approach Combines Data, Organization, Processes, and Technology Views

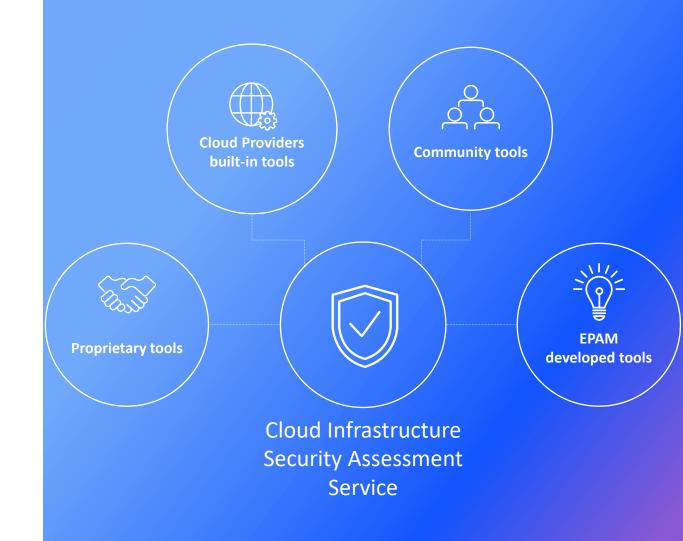
Organization Processes Organizational structure Sourcing strategy Roles and accountabilities Security management Security incident response · Functional interfacing with wider Security testing organization Vendor management Compliance and certifications Governance and awareness **Target Operating** Model **Technology Data** • Security current state and operating model Data classification Security policy, guidelines, standards, procedures Data segregation/segmentation Security architecture and framework · Data integrity, confidentiality, · Security tooling and availability Security logging and monitoring Operating model



Network security automation

Cloud Security Program Starts with Assessment

- Cloud security assessment
- Quick wins
- Continuous Cloud Security Posture Management
- Integrate security activities in SDLC, infrastructure and applications architecture, application security, security testing
- Auto remediation
- Monitoring solution & SIEM & Security Operations Center
- Governance solution, centralized dashboards
- Security certification / attestation readiness & preparation





Azure Security and Governance Assessment

Our approach to Azure security assessment is a Managed Cloud Security and Compliance Assessment. We start with the baseline assessment and continue with an iterative, continuous assessment providing ongoing posture management

Baseline Cloud Security Assessment

4-phase engagement includes:

- Assets Discovery
- Workshops and interviews with SMEs and Stakeholders
- Architecture assessment against security best practices

- Documentation review and cross-check against implementation
- Infrastructure security automation assessment
- Analysis of results: impact evaluation, verification and prioritization of findings
- Remediation roadmap preparation
- · Workshop with insights based on results and recommendation

Phase 1:

Onsite workshops and interviews

Phase 2: Scanning activities **Phase 3:**Report finalization

Phase 4:
Remediation roadmap

Iterative (Continuous) Security Assessments

The subsequent assessments would focus on a limited scope of change between releases

- New Assets Discovery
- · Workshops and interviews with SMEs and Stakeholders
- Architecture assessment against security best practices
- Documentation review and cross-check against the implementation
- Infrastructure security automation assessment
- CI/CD and SDLC assessment

Deliverables

- Approved scope and requirements agreement
- Approved assessment plan
- Assessment report answering the questions:
 - → How 'safe'?
 - → Conforms to standards and best practices?
 - → How 'scalable'?
 - → Verified non-functional requirements
 - → How efficient is the CI/CD and SDLC automation?
- Mitigation recommendations overview
- Cloud Security policy, processes updates recommendations



Timeline for Azure Security Assessment

Timeline	W1	W2	W3	W4-6	Next Steps
Security Team	PPERATATION			REPORT	
		EXECUTION			
Cloud Team				REMEDIATION	

PHASE	DESCRIPTION	DELIVERABLES	
Preparation	Gather the info from the Project Team, define scope, set up toolset	 Stakeholders identified, scope identified, all available information collected, required access granted, tools and frameworks set up. Scope and requirements are discussed Assessment plan approved 	
Execution	Automatic security check along with manual validation is performed to discover security issues	Security assessment is completedGaps and vulnerabilities identified	
Reporting	All disclosed issues are summarized and classified in Security Reports. Cloud Team knowledge transfer	 Security Assessment Report is created Mitigation recommendations are provided Results discussed and clarified with Cloud Team 	
Remediation	Mitigation recommendations are developed by Security Team and discussed with Cloud Team. Security Program Roadmap is developed	Security Program Roadmap is discussed and clarified with stakeholders	



Microsoft Solutions Partner

EPAM is recognized by Microsoft for demonstrated expertise in creating and delivering innovative solutions using Microsoft technologies to help customers solve complex business challenges.





Digital & App Innovation | Azure

- DevOps with GitHub
- Kubernetes on Azure
- Migrate Enterprise Apps to Microsoft Azure
- Low Code Application Development
- Build and Modernize Al Apps with Microsoft Azure



Data & AI | Azure

- Analytics
- Al and Machine Learning
- Infra and Database Migration



Infrastructure | Azure

Infra and Database Migration



Security

- Cloud Security
- Threat Protection



Business Applications

- Low Code Application Development
- Intelligent Automation



2023

MICROSOFT PARTNER OF THE YEAR



MSUS Winner for Migration on Azure



MSUS Finalist for Application Modernization



Global Finalist for Retail & Consumer Goods



EPAM Cyber Security Practice

EPAM Key Facts

10+
YEARS OF

EXPERIENCE

GLOBAL DELIVERY CENTERS

20+

300+

ACTIVE PROJECTS

Our Offerings

- Cloud Security
- Application Security, Secure SDLC
- Data Security

- Security Testing
- MDRS & SOC
- Governance, Risk & Compliance

Partnerships





















Highlights

- Digital, application and hybrid cloud engineering heritage
- Full spectrum combining advisory and tactical services and technologies
- Continuous improvement compliance and risk management
- Wide-and-deep research-based security expertise

Experience Across Industries

- Financial Services
- Telecom, Media & Entertainment
- Consumer
- Life Sciences & Healthcare
- Travel & Hospitality
- Industrial
- Insurance
- Software & Hi-Tech



Security Journey with EPAM + Microsoft

GOVERNANCE & COMPLIANCE, **ADVISORY**

Azure MDR as a Service

• EPAM Cloud Security

Accelerator

EPAM SOC

Security Analytics

OPTIMIZATION

• Regulatory Compliance & Regional privacy Assessments/Management

- Enterprise Security Posture Mapping
- Virtual CISO Services
- Cybersecurity Advisory Services

IMPLEMENTATION ROADMAP

- Azure Security Workshop
- Azure Security Assessment
- M365 Security Assessment
- Security testing

- Azure Security Services PoC, Pilot
- Azure Cloud Security Configuration
- Application Security / Secure SDLC
- Data Security in the Azure
- Zero Trust IAM
- EPAM SafeCloud

- Agile Security Service
- Onboarding & Training
- Incident Response

OPERATIONS

- Continuous Threat Resilience
- Secure CI/CD (Azure DevOps)
- Eye-of-The-Enemy Platform

Security Certification Preparation (SOC2, ISO 27001, HITRUST)

Based On

TALENT

PARTNERS

METHODS & FRAMEWORK

ACCELERATORS



