<epam>

EPAM Azure Security Assessment

2021

EPAM MS Azure Competency

Microsoft Azure Microsoft Gold Partner

KEY FACTS

1,000+
Azure Certifications

4,000+
Azure-Experienced Engineers

10+
Years of Partnership

20+
Delivery Centers

7
MS Azure Most Valuable Professionals

Top 10
Partner in US Driving Azure Consumption

SELECTED CLIENTS

Wolters Kluwer · COLEMAN · KOMATSU MODULAR · Chevron · unicef · Honeywell THE POWER OF CONNECTED

DENTSPLY · THOMSON REUTERS · HYPERION INSURANCE GROUP · Coca-Cola · LUXOTTICA · McKESSON

COMPETENCY FOCUS AREAS

- Gold Cloud Platform
- Gold Application Development
- Gold Application Integration
- Gold Collaboration and Content
- Gold Data Analytics
- Gold Data Platform
- Gold Datacenter
- Gold DevOps
- Gold Messaging
- Gold Security
- Gold Windows and Devices
- Silver Cloud Business Application (Gold in progress)

EPAM Security Competency

EPAM KEY FACTS

33K+
Engineers & Consultants

8K+
DevTestSecOps Professionals

300+
Security Architects, Engineers & Consultants

PARTNERSHIPS

amazon web services · Google Cloud · Microsoft Azure · CHEF · ITIL Training Organization Accredited by PEOPLECERT

Akamai · SECURONIX · splunk> · dynatrace · HashiCorp

TOOLS

VERACODE · Checkmarx · FORTIFY · BLACKDUCK · BURPSUITE

OWASP ZAP · PRISMA CLOUD · NeuVector · protegrity · Qualys

Nessus · RAPID7 · amazon web services · Microsoft Azure · Google Cloud

EXPERIENCE ACROSS INDUSTRIES

- Financial Services
- Business Information & Media
- Retail & Distribution
- Life Sciences & Healthcare
- Travel & Hospitality
- Manufacturing & Automotive
- Insurance
- Born-digital companies
- Software companies

Top critical issues that lead to security breaches in the cloud:

Unauthorized access

Misconfiguration of the cloud platform/wrong setup

Insecure interface/ APIs

Is data in the Cloud **Safe**? Are we following **best practices**? Are we **Ready to Release**?

ARE WE SAFE?

- Are our customers and their data safe?
- Are we secure?
  - Secure configuration
  - IAM/CIAM, Network, Kubernetes, Databases etc
  - Data Protection, Secret Management
- Are we compliant with standards and regulations (SOC 2, HIPAA, ISO 27001, GDPR, CCPA, PCI DSS) ?

EPAM Cloud Security Assessment

Quick and practical way of taking control on cloud security using proven DevTestSecOps approach:

- EPAM Cloud Security Assessment provides a quick way to assess the current cloud security posture, provides analysis and report prioritized and categorized list of issues.
- Cloud Security Assessment informs the Roadmap for highly automated solutions and security programs for the cloud

Cloud Security Breach: Potential Business Impacts

Businesses vigorously look for the new revenue streams to offset the negative consequences of **COVID-19** and seize the opportunity in the rapidly changing environment. The speed of adoption of cloud and digital solutions are key to survival and competitive advantage.

Overstretched IT and Security operations are in a **perfect storm:** technical debt created over years has inflated the impact on business operations and **security risk**. All familiar and brand-new security risks are raised disproportionally due to drastic changes in IT and cloud operations related to work from home.

→ **It is the worst time to get a security breach that is usually accompanied with:**

LOSS OF CUSTOMERS

- Loss of customer trust: majority will not do business with a company that failed to protect the data

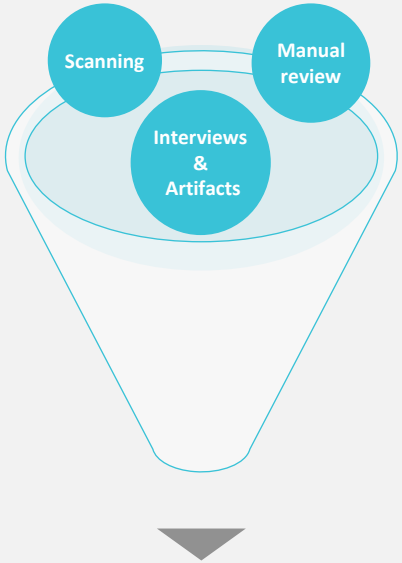
BRAND IMAGE IMPACT

- Direct loss of business
- Devaluation of the brand
- Ability to attract the best talent, suppliers, and investors

DIRECT FINANCIAL LOSSES

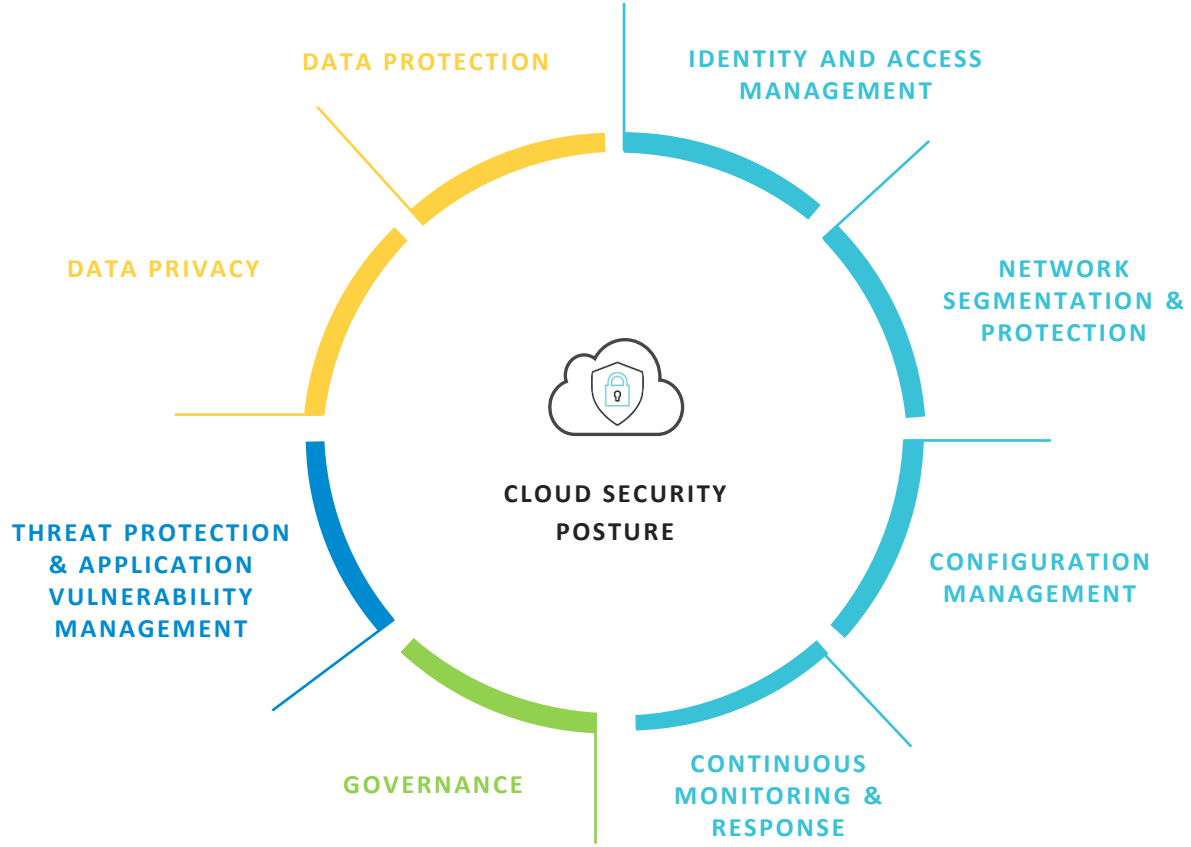
- Direct financial losses as a result of a theft
- Monetary penalties/fines for businesses

Holistic Approach to Cloud Security



Report:

gaps, recommendations, roadmap



Azure Cloud Infrastructure Assessment

DESCRIPTION

3-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
- CI/CD and SDLC assessment

Phase 1:	Phase 2:	Phase 3:
Onsite workshops and interviews	Offsite analysis	Finalize report and onsite playback

TEAM COMPOSITION

- Cloud Security Architect
- Cloud Security Engineer

Microsoft Azure

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

KEY ASSUMPTIONS

- Customer representatives are available as required
- EPAM personnel will be granted a Read-Only access to infrastructure

Timeline for Azure Security Assessment

PHASE	DESCRIPTION	DELIVERABLES
Preparation	Gather the info from the Project Team, define scope, set up tool-set.	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 completed. Issues identified.
Reporting	All disclosed issues are summarized and classified in Security Reports. Cloud Team knowledge transfer.	Security Assessment Report and Threat Model are created. Mitigation recommendations are provided. Report presentation meeting is conducted. Results discussed and clarified with Cloud Team.
Next Steps	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.

<epam>

Thank you