Azure Security Assessment

Microsoft
Solutions Partner
Security

Why You Need a Security Assessment for Your Azure Environment

As cloud adoption accelerates, so do the threats that target cloud infrastructures. Many organizations assume that by migrating to Azure, they are automatically secure. However, misconfigurations, unused services, outdated policies, and insufficient monitoring can all leave your environment vulnerable.

A professional security assessment helps bridge this gap by providing an **objective, expert-driven evaluation** of your current security posture. It identifies hidden risks, verifies compliance readiness, and provides a roadmap to align with frameworks like **Zero Trust** and **Microsoft's security benchmarks**.

Key Benefits of ITX360's 5-Day Azure Security Assessment

✅ **Proactive Risk Identification**

Detect misconfigurations, access control weaknesses, and outdated components *before* they are exploited.

✅ **Compliance and Governance Readiness**

Ensure your environment aligns with regulatory requirements such as GDPR, ISO 27001, or industry-specific mandates.

✅ **Zero Trust Architecture Alignment**

Gain tailored recommendations to evolve your environment toward a Zero Trust security model — the modern gold standard for access control and segmentation.

✅ **Actionable Recommendations**

Receive detailed reports with prioritized, actionable insights to remediate vulnerabilities and strengthen defenses.

✅ **Optimized Security Investment**

Understand which Azure-native or third-party tools are underutilized or misconfigured, so you can maximize ROI.

✅ **Enhanced Visibility and Control**

Improve security monitoring, alerting, and incident response capabilities by evaluating existing tools and processes.

ITX360's 5-Day Azure Security Assessment.- Plan

First 3 days – Plan

Agenda

- Introduction to ITX360 Azure expertise.
- Definition of Scope for assessment
- Current Azure Architecture and Business review.
- Azure Resource Analysis.
- Review and Categorize IAAS, PAAS, SAAS service.
- Discuss the Compliance requirements as an organization.
- Verify the Security product and solution operation under Azure environment.

Deliverables

- Logical Network Diagram
- Current environment Security Score based on the required Security compliance.
- Report of Azure Resources and Security Product running on Environment

Last day 2 -Plan

Agenda

- Assess Best Practices and Recommendations for Azure Resources
- Review Network Setup in Line with Zero Trust Principles.
- Asses Verify the Configuration of Network Security Appliance Firewall, Application Gateway, Load Balancer, NSG, Private Endpoints and Service Endpoints.
- Asses Patch management and endpoint protection on Servers
- Review Security Baseline for SaaS and PaaS Services
- Disaster Recovery and Backup Plan Evaluation
- Monitoring Systems and Security Incident Management.

Deliverables

- **Recommended Network Security logical Architecture**.
  - A comprehensive, optimized network security architecture to meet Zero Trust standards.
- **Security recommendation report for Azure Resources which aim to Zero Trust Framework.**
  - A security recommendation report for Azure resources focused on Zero Trust principles.
- **Security recommendation report for Azure Network Security Appliance.**
  - A report detailing recommendations for network security appliances in your Azure environment.
- **Recommended Alerting and Monitoring Configuration Report.**
  - A report on the recommended alerting and monitoring setup to enhance security oversight

ITX360

LET'S TALK TECH

Email : cloudsales@itx360.com

Phone: +94777270822