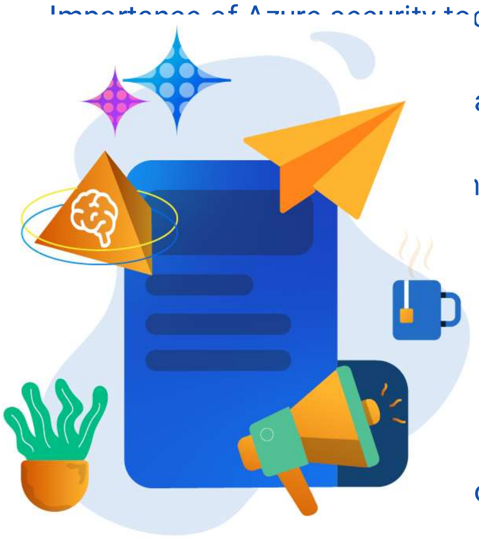
Cyber Security

Azure Security Services Checklist | A Quick Guide

Navdeep Singh Gill | 16 February 2023

Table of Content

In this Article



Microsoft Azure Managed Services

Cloud Security Services and Solutions Consulting

Azure Sentinel Managed Services and Cloud Native SIEM

Introduction to Azure Security Services

Azure is a hybrid cloud service platform. It supports various operating systems, computing languages, architectures, resources, applications, and computers. This will manage Docker-integrated Linux containers; develop Html, Python, .NET, PHP, Java, and Node.js apps; and develop backends for iOS, Android, and Windows computers. With more and more enterprises shifting to the cloud, there lies a definite need for its Security. Are there any Azure Security Services around? Luckily, you have reached the right place.

Why is Azure Cloud Security Important?

Cloud storage eliminates the need to build data centers and invest in costly equipment. Businesses are switching rapidly to cloud technology to speed up innovation and encourage collaboration. This is where its Services come into the picture. It is a procedure and technology that secure the cloud computing environment against cyberattacks.

Importance of Azure security tools

Azure provides tools and capabilities for security to create a secure platform. Confidentiality, integrity, availability of customer data, and enabling transparent accountability - It takes care of everything. Basically, the cloud provides significant benefits in addressing significant threats to information management. In an on-site environment, organizations are likely to have unfulfilled responsibilities and limited resources available to invest in security, creating an environment where attackers can exploit vulnerabilities at all layers. One of the cloud's keys to data security is to prepare for future environments in which the data may exist and what protections are required for that state. For its data security and encryption best practices, the recommendations are around the services discussed below.

> Governance policies contain a set of protocols of how things should be regulated on the cloud.Click to explore about, Click to explore about, Cloud Governance

What are the various Azure Managed Security Services?

In the subsequent section, we will elaborate on the 7 Best Services for Azure Security.

General Security

The list of general Azure Security Technologies is below:

i. **Security Center**: It is a workload protection solution; it provides security management. Additionally, advanced threat protection across the hybrid cloud.

ii. **Key Vault**: It secures every sensitive detail like passwords, connection strings, and other information you need to keep your apps working.

iii. **Monitor logs**: A service that collects telemetry and other data and provides a query language and analytics engine to deliver operational insights for apps and resources. It can be used standalone or along with Azure Security Centre.

iv. **Dev/Test Labs**: A service that helps testers and developers instantly create Azure environments while minimizing waste and controlling.

Operations Security

The list of Operations Security technologies is below:

i. **Security and Audit solution**: It provides a complete view of an organization's IT security posture

ii. **Resource Manager**: It enables us to work with the resources in the organization's solution as a group. In a single coordinated operation, an organization can deploy, update, or delete all the resources.

Applications Security

The list of technologies involved is below:

i. **Web Application vulnerability scanning**: It provides one-click vulnerability scanning.

ii. **Web Application Firewall**: The web application firewall (WAF) in Azure Application Gateway aims to secure web apps from rising web-based threats such as SQL injection, cross-site scripting threats, and user hijacking.

iii. **Application Insights**: It is for web developers, an extendable Application Performance Management (APM) program.

Data Catalog enhances old investments' performance, adding metadata and notation around the its environment's data.Click to explore about, Click to explore about, Azure Data Catalog

Storage Security

Listed below are the technologies:

i. **Role-Based Access Control (RBAC):** Restricting access based on the need-to-know and least-privilege principles is imperative for organizations that want to enforce security policies for data access.

ii. **Encryption**: Encryption in transit is a mechanism for protecting data when it is transmitted across networks.

Network Security

Listed below are the technologies:

i. **Virtual Network**: An Azure virtual network (VNet) represents a client's network in the cloud. It is a logical isolation of its network fabric dedicated to your subscription.

ii. **VPN Gateway:** VPN gateway is a virtual network gateway that sends encrypted traffic across a public connection.

iii. **Network Layer Controls**: Network access control is the act of controlling connectivity to and from individual devices or subnetworks, forming the center of network security.

Backup and Disaster Recovery

The two types of Disaster Backup Recovery are listed below:

i. **Site Recovery**: It helps to orchestrate Backup, failover, and recovery of workloads and applications. Whenever the primary location goes down, they would be accessible from a secondary site.

ii. **Virtual machine backup**: Azure Backup protects application data with minimal operating costs and zero capital investment.

Know about our Services in Disaster Backup Recovery here.

Identity and Access Management

There are two categories of Identity and access management:

i. **Active Directory**: The authentication repository supports its multi-tenant, cloud-based directory and multi-identity management services.

ii. **Multi-Factor Authentication**: A security provision that utilizes several authentications and verification methods before accessing protected information.

Sentinel can collect data on all users, devices, applications, and infrastructure both on-premises and across multiple cloud environments.Click to explore about, Click to explore about, Sentinel and its Components

Azure Security best practices checklist

Check out our Azure Security Services Checklist for better securing the data on it.

The Starting Checklist

1. Ensure that multifactor authentication is enabled for all users
2. Ensure that there are no guest users.
3. Use Role-Based Access Control to manage access to resources.
4. Ensure that ‘enable users to memorize multifactor authentication on devices they trust’ is disabled.
5. Ensure that the ‘number of processes required to reset’ is set to 2.
6. Make sure that the ‘number of days before users are asked to re-confirm their authentication report’ is not set to 0.
7. Assure that ‘caution users on password resets’ is set to yes.
8. Ensure that ‘notify all admins when other admins reset their password?’ is set to yes.
9. Ensure that ‘users can comply with apps obtaining company data on their account’ is set to none.
10. Guarantee that ‘users can add gallery apps to their Entrance Panel’ is set to no.
11. Ensure that ‘users can disclose applications’ is fixed to no.
12. Guarantee that ‘guest users agreements are limited’ is set to yes.
13. Ensure that ‘members can request’ is set to no.
14. Guarantee that ‘guests can invite’ is set to no.

15. Ensure that entrance to the Azure AD administration portal should be limited.

16. Integrate Security Center alerts for SIEM solutions.

17. Use the shared responsibility model to your advantage.

The Ending Checklist

1. Ensure that ‘users can create security associations’ is set to none.

2. Ensure that ‘self-service group administration enabled’ is established to no.

3. Make sure ‘users who can handle security groups’ is set to none.

4. Ensure that ‘users can create Office 365 groups’ is set to no.

5. Ensure that ‘users who can manage Office 365 groups’ is set to none.

6. Make sure ‘require multi-factor auth to join devices’ is set to yes.

7. Ensure that ‘secure transfer required’ is arranged to enable.

8. Ensure that ‘storage service encryption is set to enabled

9. On SQL servers, ensure that ‘auditing’ is set to on.

10. On SQL servers, ensure that the ‘auditing type’ is set to a blob.

11. Ensure on SQL servers that ‘threat detection is set to on.

12. On SQL servers, ensure that ‘threat detection types’ is set to all.

13. On SQL servers, ensure that ‘send alerts to’ is set.

14. Ensure on SQL servers that’ email service and co-administrators are enabled.

15. On SQL servers, ensure that firewall rules are set as appropriate.

16. Disable RDP access on network security groups from the internet

17. Disable SSH access on network security groups from the internet

Want to know about the services we offer in Cloud Security? Explore our Cloud Security Services and Solutions here.

Conclusion

The Azure platform continuously evolves, offering many new features without extra cost. The Virtual Network Endpoint feature is there for many of its services, it becomes interesting to review our deployed applications to improve their security. Today organizations are adopting cloud services rapidly. This is why leveraging Microsoft's power helps organizations become more agile, competitive, and innovative.

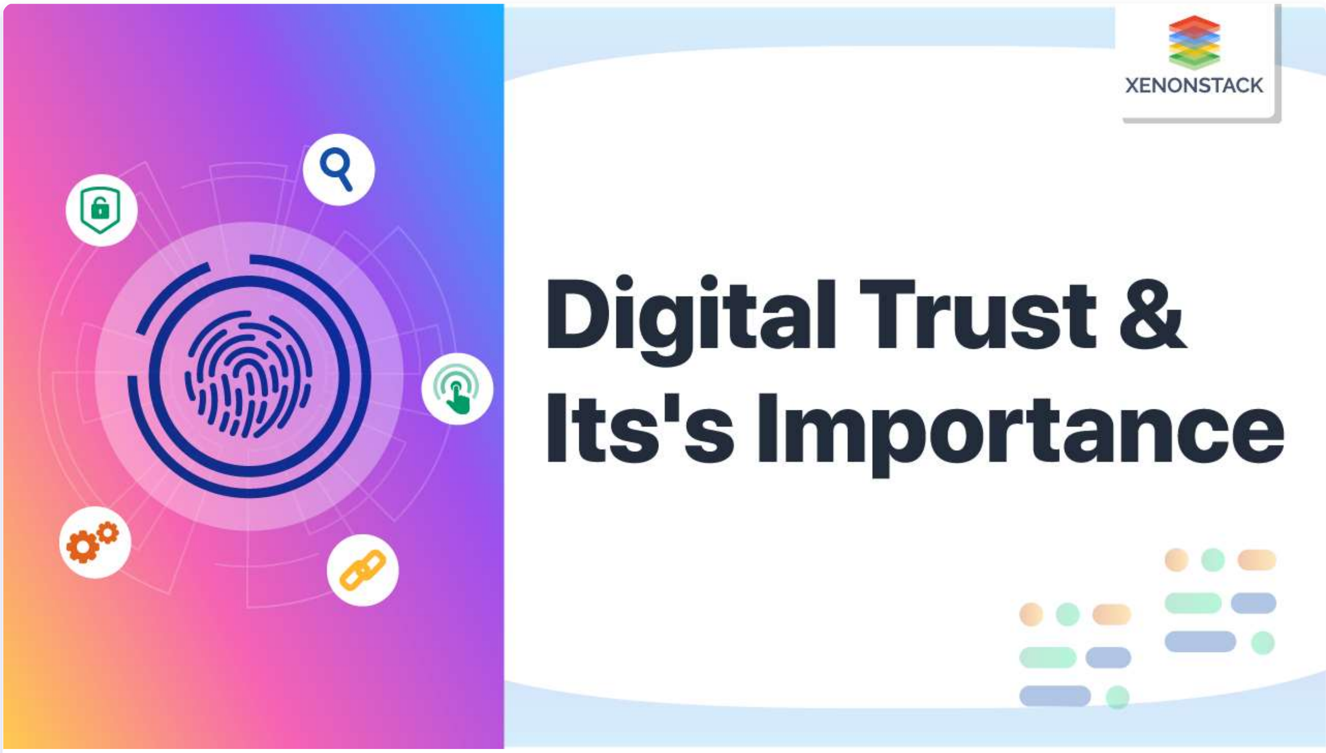
- Discover more about Cyber Security Services and Solutions
- Explore More about Sentinel Managed Services and Cloud Native SIEM

Related Articles

Cyber Security

Zero Trust Security Architecture

19 May 2023



Cyber Security

Digital Trust | Complete Guide

29 May 2023

Cyber Security

What is Machine Learning (ML) in Security? - A Quick Guide

28 April 2023

How is Generative AI transforming different industries and redefining customer-centric experiences?

Explore How

XENONSTACK

Company

About Us

Neural Company

Company Blog

Careers at XenonStack

Contact Us

Cloud Native

DevOps

Kubernetes

Observability

Serverless

Application Modernisation

Data Engineering

Graph Analytics

IoT

Real-Time Analytics

LakeHouse

Cloud Datawarehouse

AI Engineering

Computer Vision

Enterprise Search

MLOps

Conversational AI

Robotic Process Automation

Cloud Platform

UI Engineering

Video Analytics

Cloud Security

Cloud Native App

Platform Engineering

Solutions

DataOps

SRE Managed

Managed Analytics

Managed AI Cloud

Managed SOC

We are members of :

Partnerships & Certifications :

kubernetes
SERVICE PROVIDER

System Status

Cookie Manager

Terms of Use

Security Policy

Trademark Policy