Security in Microsoft Azure

Virtualization and Cloud Computing

APRIL 13, 2020

SUBMITTED BY: M. IFTIKHAR UDDIN KHAN SAMI
022-16-113275

Submitted by: M. Iftikhar Uddin Khan Sami (022-16-113275)

Contents

Submitted by: M. Iftikhar Uddin Khan Sami (022-16-113275)

Assignment- Briefly discuss how Microsoft Azure provides security?

Security is integrated into every aspect of Azure. Azure offers you unique security advantages derived from global security intelligence, sophisticated customer-facing controls, and a secure hardened infrastructure. This powerful combination helps protect your applications and data, support your compliance efforts, and provide cost-effective security for organizations of all sizes.

Introduction:

We know that security is job one in the cloud and how important it is that you find accurate and timely information about Azure security. One of the best reasons to use Azure for your applications and services is to take advantage of its wide array of security tools and capabilities. These tools and capabilities help make it possible to create secure solutions on the secure Azure platform. Microsoft Azure provides confidentiality, integrity, and availability of customer data, while also enabling transparent accountability.

Azure- An Intro:

Azure is a public cloud service platform that supports a broad selection of operating systems, programming languages, frameworks, tools, databases, and devices. It can run Linux containers with Docker integration; build apps with JavaScript, Python, .NET, PHP, Java, and Node.js; build back-ends for iOS, Android, and Windows devices.

Azure public cloud services support the same technologies millions of developers and IT professionals already rely on and trust. When you build on, or migrate IT assets to, a public cloud service provider you are relying on that organization's abilities to protect your applications and data with the services and the controls they provide to manage the security of your cloud-based assets.

Azure's infrastructure is designed from facility to applications for hosting millions of customers simultaneously, and it provides a trustworthy foundation upon which businesses can meet their security requirements.

In addition, Azure provides you with a wide array of configurable security options and the ability to control them so that you can customize security to meet the unique requirements of your organization's deployments. This document helps you understand how Azure security capabilities can help you fulfill these requirements.

Azure security documentation

Azure includes the following levels of Securities.

Fundamentals

Includes Azure security technical capabilities, Shared responsibilities for cloud computing, Security controls for Azure services, etc.

Developers

Includes Secure development best practices, Develop a secure web app, Microsoft Threat Modeling tool, etc.

Benchmarks and recommendations

Includes Azure cloud security benchmark, Azure Security Center recommendations, etc

Secrets and keys

Includes What is Azure Key Vault?, Set and retrieve a secret, What is Azure Dedicated HSM?, etc.

Data protection

Includes Data Encryption-at-Rest, Data security and encryption best practices, Storage security, etc.

Identity management

Includes Choose the right authentication method, Securing your identity infrastructure, Security best practices

Security monitoring

Includes Onboard your subscription to Security Center, Just-in-time virtual machine access, Working with security policies

IoT security monitoring

Includes Introducing Azure Security Center for IoT, Azure Security Center for IoT architecture, Get started with Azure Security Center for IoT, etc.

Security analytics

Includes What is Azure Sentinel preview?, Onboard Azure Sentinel preview, Get started with Azure Sentinel preview, etc.

Threat protection

Includes Security alerts in Azure Security Center, Advanced Threat Protection for Azure Storage, Advanced Threat Protection for Azure SQL Database, etc.

Logging and auditing

Includes Azure logging & auditing, Management and monitoring overview, etc.

Network security

Includes Security overview, Security best practices, DDoS Protection

Infrastructure security

Includes Azure facilities, premises, & physical security, Network architecture, Customer data protection, etc.

Virtual machine security

Includes Security overview, Best practices for IaaS workloads, Security configuration recommendations

Database security

Includes Data security, Best practices for PaaS databases, Security checklist

Governance and compliance

Includes Azure Policy service, Azure Blueprints service, etc.

General Azure security

Service	Description
Azure Security Center	A cloud workload protection solution that provides security management and advanced threat protection across hybrid cloud workloads.
Azure Key Vault	A secure secrets store for the passwords, connection strings, and other information you need to keep your apps working.
Azure Monitor logs	A monitoring service that collects telemetry and other data, and provides a query language and analytics engine to deliver operational insights for your apps and resources. Can be used alone or with other services such as Security Center.
Azure Dev/Test Labs	A service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost.

Storage security

Service	Description
Azure Storage Service Encryption	A security feature that automatically encrypts your data in Azure storage.
StorSimple Encrypted Hybrid Storage	An integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.
Azure Client-Side Encryption	A client-side encryption solution that encrypts data inside client applications before uploading to Azure Storage; also decrypts the data while downloading.
Azure Storage Shared Access Signatures	A shared access signature provides delegated access to resources in your storage account.
Azure Storage Account Keys	An access control method for Azure storage that is used for authentication when the storage account is accessed.
Azure File shares with SMB 3.0 Encryption	A network security technology that enables automatic network encryption for the Server Message Block (SMB) file sharing protocol.
Azure Storage Analytics	A logging and metrics-generating technology for data in your storage account.

Database security

Service	Description
Azure SQL Firewall	A network access control feature that protects against network-based attacks to database.
Azure SQL Cell Level Encryption	A database security technology that provides encryption at a granular level.
Azure SQL Connection Encryption	To provide security, SQL Database controls access with firewall rules limiting connectivity by IP address, authentication mechanisms requiring users to prove their identity, and authorization mechanisms limiting users to specific actions and data.
Azure SQL Always Encryption	Protects sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases.
Azure SQL Transparent Data Encryption	A database security feature that encrypts the storage of an entire database.
Azure SQL Database Auditing	A database auditing feature that tracks database events and writes them to an audit log in your Azure storage account.

Identity and access management

Service	Description
Azure Role Based Access Control	An access control feature designed to allow users to access only the resources they are required to access based on their roles within the organization.
Azure Active Directory	A cloud-based authentication repository that supports a multi-tenant, cloud-based directory and multiple identity management services within Azure.
Azure Active Directory B2C	An identity management service that enables control over how customers sign-up, sign-in, and manage their profiles when using Azure-based applications.
Azure Active Directory Domain Services	A cloud-based and managed version of Active Directory Domain Services.
Azure Multi-Factor Authentication	A security provision that employs several different forms of authentication and verification before allowing access to secured information.

Backup and disaster recovery

Service	Description
Azure Backup	An Azure-based service used to back up and restore data in the Azure cloud.
Azure Site Recovery	An online service that replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location to enable recovery of services after a failure.

Networking

Service	Description
Network Security Groups	A network-based access control feature using a 5-tuple to make allow or deny decisions.
Azure VPN Gateway	A network device used as a VPN endpoint to allow cross-premises access to Azure Virtual Networks.
Azure Application Gateway	An advanced web application load balancer that can route based on URL and perform SSL-offloading.
Web application firewall (WAF)	A feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities
Azure Load Balancer	A TCP/UDP application network load balancer.
Azure ExpressRoute	A dedicated WAN link between on-premises networks and Azure Virtual Networks.
Azure Traffic Manager	A global DNS load balancer.
Azure Application Proxy	An authenticating front-end used to secure remote access for web applications hosted on-premises.
Azure Firewall	A managed, cloud-based network security service that protects your Azure Virtual Network resources.
Azure DDoS protection	Combined with application design best practices, provides defense against DDoS attacks.
Virtual Network service endpoints	Extends your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

Summary of Azure security capabilities

Features to secure the Azure platform

The following features are capabilities you can review to provide the assurance that the Azure Platform is managed in a secure manner. Links have been provided for further drill-down on how Microsoft addresses customer trust questions in four areas: secure platform, privacy & controls, compliance, and transparency.

Secure Platform	Privacy & Controls	Compliance	Transparency
Security Development Cycle, Internal audits	Manage your data all the time	Trust Center	How Microsoft secures customer data in Azure services
Mandatory Security training, background checks	Control on data location	Common Controls Hub	How Microsoft manage data location in Azure services
Penetration testing, intrusion detection, DDoS, Audits & logging	Provide data access on your terms	The Cloud Services Due Diligence Checklist	Who in Microsoft can access your data on what terms
State of the art data center, physical security, Secure Network	Responding to law enforcement	Compliance by service, location & Industry	How Microsoft secures customer data in Azure services
Security Incident response, Shared Responsibility	Stringent privacy standards		Review certification for Azure services, Transparency hub

Product and Services

Related products and services

Security Center

Unify security management and enable advanced threat protection across hybrid cloud workloads

Application Gateway

Build secure, scalable and highly available web front ends in Azure

Azure Active Directory

Synchronise on-premises directories and enable single sign-on

Azure DDoS Protection

Protect your applications from Distributed Denial of Service (DDoS) attacks

Key Vault

Safeguard and maintain control of keys and other secrets

Azure Information Protection

Better protect your sensitive information—anytime, anywhere

References:

- ✓ https://docs.microsoft.com/en-us/azure/security/fundamentals/services-technologies
- ✓ https://docs.microsoft.com/en-us/azure/security/
- ✓ https://docs.microsoft.com/en-us/azure/security/fundamentals/overview
- ✓ https://docs.microsoft.com/en-us/azure/security/fundamentals/overview#features-to-secure-the-azure-platform