# Describe the concepts of security, compliance, and identity (10-15%)

# Describe the capabilities of Microsoft identity and access management solutions (25-30%)

# Describe the capabilities of Microsoft Security solutions (25-30%)

# Describe the capabilities of Microsoft compliance solutions (25-30%)

**Cyber Security Concepts**

Gain illegal access to computer to cause damage or harm.

Global economic and social disruption

Cyber security – Technology,process and training – helps protect systems, nw, program and data.

Cyber security – Achieve Confidentiality, Integrity and Availability (**CIA**)

**Confidentiality** – Information visible only to the right people

**Integrity** – Information to be changed by the right people or processes

**Availability** – Information must be visible and accessible whenever needed

Threat Landscape – Email, Social Media acc, Mobile devices, Tech infra, Cloud services, People

Malware – Malicious + Software. Software used by cyber criminals to infect systems and carry out actions

Malware – Steals data. Disrupts normal usage and processes.

Malware components – Propagation (How it spreads) and Payload

**Propagated as below – 3 types**

Malware -> Virus, Worms, Trojans

Virus – Means of entry required, can cause harm once inside.

Worm – No user action required. Worm finds vulnerable systems. Spreads to other systems.

Trojan – Pretending to be genuine. Secretly performs malicious actions like stealing information.

**Payloads as below – 4 types**

Malware – Ransomware, Spyware, Backdoors, Botnet

Ransomware – Locks systems, asks ransom. Encrypts

Spyware – Spies on devices. Keyboard scans, collecting passwords and transmitting back to attacker

Backdoor – Bypass existing security measure via exploit. Hiding malicious code in software. This is backdoor

Botnet – Group of infected devices. Like crypto miners

**Mitigation Strategies – 4 types**

MFA, Browser Security , User education, Threat intelligence,

MFA – Multiple forms of identification.

Browser security – Uptodate, unauthorized extension removal,, block sites

Education – Training

Threat intelligence – Policies for security devices, user access and more.

Cryptography -

Encryption – combine large random prime numbers to create keys.

Asymmetric Encryption – public and private keys

UserA and UserB has public keys

UserA uses UserB’s public key and encrypts. UserB uses its private key to decrypt.

Types of Encryptions –

**DES** Data Encryption Standard, **Triple DES**. – one of the first symmetric encryption std.

**AES** Advanced Encryption Standard – Replaced DES

**RSA**. – One of the first asymmetric encryption standard

Hashing – Verifying data like documents and images and see if it’s tampered with.

Hashing uses algorithm known as **hashing function**.

Hashing function – Converts the original text to unique fixed length value called **hash value**

Each time the text is hashed – same value is produced. This hash will be used as unique identifier

Hashing is not encryption.

Hashing does not use keys

Hashed value cannot be decrypted back to original

Hash Function – SHA. Secure Hash Algorithm. Produces hash value of 256 bits long.

**Digital Signing – Requires digital signing service. Like Docu Sign and Adobe Sign**

Uses asymmetric key pair.

Used to prove the document is not changed

Uses private to prove the identity since no one has that private key

User A signs publicly available hash algorithm – Creates Hash

Encrypts the Hash using his private key and attaches it to the document as document signature

User A send it to User B

User B creates Hash using publicly available Hashing algorithm

Decrypts the signature using User A’s public key

If the decrypted signature matches the hash of the document, then document is not changed

Digital Certificates

Issued by CA. Verify identity subject.

Data in certificate includes – subject information, subjects public key

Certificate links user A identity with the public key.

Authentication based attacks

Brute force, dictionary, credential surfing, keylogging, social engineering (Phishing, pretexting,Baiting)

**Authorization Security Techniques** – Conditional access, Least privileged access, Lateral movement, zero trust

**Zero Trust – Never trust. Always verify**

Verify explicitly – Each request is fully authenticated and authorized. (MFA + CA)

LPA – Authorize only with minimum rights

Assume breach – Additional layers of security.

Common Network Attacks

Man in the middle – intercepting the packets

DDoS – compromise availability of services

Common Wireless attacks

Wardriving – Attacker searches for unsecuried wifi.Uses the compromised network

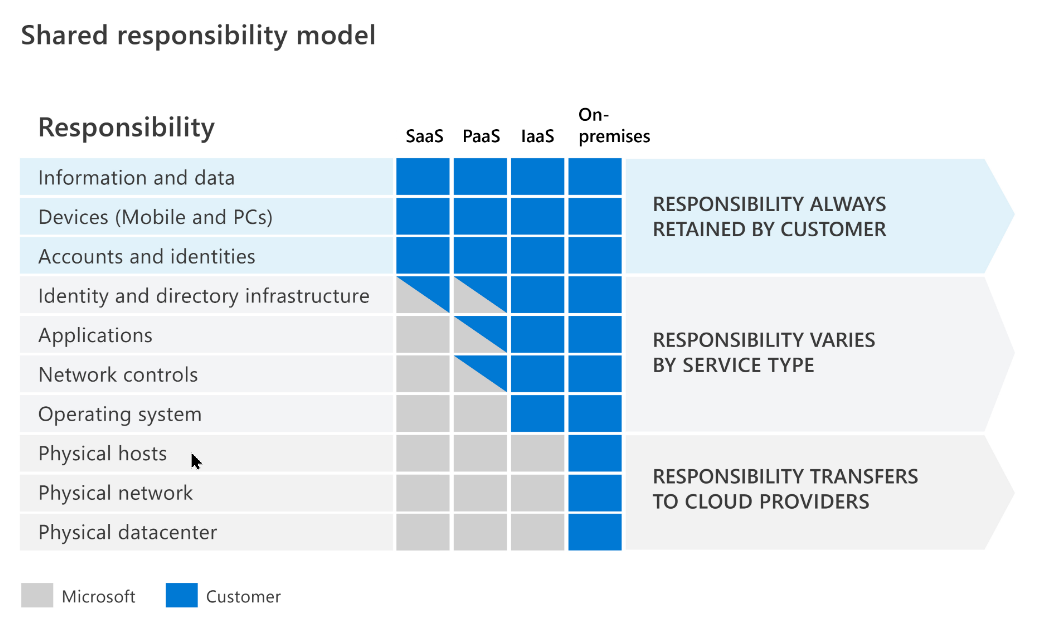
Spoofing wifi hotspots – free wifi attack

Session replay attack – stealing cookies

A zero-day vulnerability is any flaw that is previously unknown to the application owner and unpatched.

Shared Responsibility model

In cloud responsibility is shared between customer and cloud provider



SaaS – Cloud provider is responsible for everything except Data, Devices, Accounts and Identities

Responsibilities always by customer – Data, devices, Accounts and identities

**Describe Defense in Depth**

Layered approach to slow the advance of the attack.

Each layer provides protection. One layer breached the next layer will prevent

1. Physical – Limit DC access
2. Identity and access – MFA or Conditional based access
3. Perimeter – DdoS
4. Network – Network segmentation and Network ACL
5. Compute – Access to VM. Port Security
6. Application – Vulnerability management
7. Data – Encryption of data

**Zero Trust guiding principles**

Verify Explicitly

Least privilege access – Just In Time, Just Enough Access

Assume breach – NW segmentation, user, dev, apps. Encryption, analytics

**6 foundational pillars in Zero Trust – IDADIN**

* Identity – Verify with strong authentication
* Devices – Monitor for compliance
* Applications – Manage permission and access. Discover apps
* Data – Classify, label, encrypt.
* Infrastructure – Assess versions, configs and JIT access. Use telemetry to detect attacks. Block or tag risky behavior
* Networks – Segment. RTTP, End to end encryption, monitoring, and analytics

Identity has become the new security perimeter.

An identity may be associated with a user, an application, a device or something else.

Four pillars of identity

1. Administrator
2. Authentication
3. Authorization
4. Auditing

**Role of Identity Provider**

Modern authentication – Token and information is stored and managed by the identity provider.

The centralized idp is supplying the authN service

Cloud based authN provider – Azure AD. Twitter, Google, Amazon, LinkedIn and GitHub

Single Sign-On -

Federation – SSO between multiple Identity Providers

AD –

AD DS doesn’t natively support Mobile devices, SaaS apps, LOB apps that require modern authN

Federation – Trust is not always bidirectional

Azure AD DS – IdaaS Identity as a service – Solution for apps across cloud and on premise

Azure AD provides API – Allows developers to build personalized app using existing organizational data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Azure AD Free | Office 365 Apps | Azure AD P1 | Azure AD P2 | Pay as you go |
| Sync on prem  Basic reports  Self service password change for cloud users  SSO across Azure, m365 and SaaS apps | All in Free + Self service password reset for cloud users  Device Write back  AD is with 365 E1,3,5, F1 and F3 | Dynamic Groups  Self service group mgt  MS identity manager (On premise identity and access management suite)  Cloud Writeback – SSPR for on premise users | All P1  Azure AD IDP  Conditional Access to your apps and company data  PIM – help discovery, restrict and monitor administrators and their access.  Just In Time access | Azure B2C – ID and access mgt for customer facing apps |

Employees and Guests are both called Users in Azure AD

**Azure B2B** – Collaboration. External identity feature – Can add Guest User

Organization can securely share apps and services with guest users from another organization

**Azure AD Identity Types**

|  |  |  |  |
| --- | --- | --- | --- |
| User | Service Principal | Managed Identity | Device |
| Employees and guest  B2B – External Identities  B2B collaboration – securely share apps and services with guest users from other organization | Identity for an application  If application needs to delegate its Identity and access functions to azure ad.  App to register with azure AD for enabling integration  After registration SP is created in each Azure AD where app is used.  Enables authN and authZ  Developers must manage and protect SP credential | Same like SP but developers don’t need to manage it  Provides an identity for apps to use  Resources must support Azure AD authentication  No cost  Types – System assigned & User Assigned  **System Assigned** – Tied to the life cycle of the service instance.  If resource is deleted, azure automatically deletes the identity  Only Azure resource can use this identity to request tokens from azure AD  Cannot be shared  **User Assigned**  Standalone azure resource  Assigned to one or more instances of azure service.  Identity is managed separately from the resources  Can be shared | Mobile, laptop, server or printers.  **Azure AD registered devices** BYOD  No organizational account required  Win10, IOS, Android, MacOS  **Azure AD Joined**  Joined via Organizational account.  Owned by organization  Win 10 except home,  Win server 2019 VM running in azure  **Hybrid Azure AD Joined**  Need Organizational account to sign in |
|  |  |  |  |

Graphical user interface, text, application, email

Description automatically generated

To enable single sign to cloud based resources – register and join devices to Azure AD

Azure Ad Joined devices can SSO to resources and apps that rely on on prem AD

MDM and MAM – Microsoft Intune

**Types of External Identities**

External Identities - Access to organization’s apps and data to external users. Bring Their Own Identities BTOI

External IDP – Azure AD tenant, Facebook, google or Enterprise Identity Providers

Using the above, customers and partners can use their own identity to access apps

Federation is created by our Admin to the External Identity Providers

**2 types of Azure AD External Identities**

B2B - Share your apps and resources with external users

B2C - Identity Management solution for consumer and customer facing apps

|  |  |
| --- | --- |
| B2B collaboration- Premium P1 and P2 | B2C Access Management - Premium P1 and P2 |
| Share org apps and services with external people  We maintain our own Data control  Uses Invitation and redemtption process  Self service sign up user flow can be enabled  User who signup will be shown as guests in Azure AD  SSO to all Azure AD connected apps are supported  Guests can be added to same groups as employees | Customer IDM solution.  External users can sign in with their social, entreprise, or local account identities to get SSO.  Supports millions of users  Billions of authentications per day  Scaling and safety is taken care  Monitoring, DDoS, password spray, or Brute force  External users are managed in the Azure AD B2C directory  Separated from organization employee and partner dir.  SSO to customer owned apps within the azure AD B2C  Branding can be done |

**Hybrid Identity**

Requires – On Premise AD, Azure AD connect – Bridges to azure AD

|  |  |  |
| --- | --- | --- |
| Azure AD Password Hash Sync | Azure AD Pass through authentication | Federated Authentication |
| Enable authentication for on premise directory objects in Azure AD  Azure AD handles Users sign in process  Password hash is extracted from on prem A using Az AD Connect  Synched to Azure AD authentication service  Enables user authentication to take place against Azure AD  Highly available cloud authentication benefit.  On Premise users can authenticate with azure ad to access cloud based apps. Even if AD DS is down. | Enable users to sign in to both on prem and cloud based app using same password.  When users sign in – PTA validates users password directly against AD DS.  No password validation in cloud.  Good for enforcing on premise AD security and password policies  Azure Ad connect needs 1 or more authentication agents  Azure AD will encrypt user password with public key of authentication agent.   * On prem agent retrieves the uname and encrypted password from azure ad * Decrypts the password with its private key * Validates the uname and pass against AD DS   AD DS evaluates and respond to agent  Agent Notifies Azure AD  If authentication agent fails then No Office 365 login possible | Used by organizaitons with advanced features not supported in Azure AD  Smart card or cert based SSO  SSO via on prem MFA server  SSO via 3rd party authenticaton solution  Azure AD hands off authN process to services such as AD FS for password validation.  All authN occurs on premise  Uses AD connect + additional servers  Larger infra required  Org, can setup PHS as backup if AD FS fails |

Azure AD supports 2 Phone authentications – SMS and Voice call verification

Voice call verification – During SSPR or Azure AD MFA

Authentication Methods – 3 types of methods.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Phone based | OAUTH | Password less | Password less | Password less | Password less |
| SMS  Voice call verification | **Open Auth**  Time Based One Time Password  Software or Hardware  Only supported as secondary forms of authentication.  Verified during SSPR or Azure AD MFA | Biometrics – Hello4Business  FIDO2 Security keys | **Hello4Business**  Combination of key or certificate tied to device  + PIN or biometrics  Uses private key to cryptographically sign data which is sent to IDP  Protects against  **Credential theft**  Can be used as MFA authenticaton | **FIDO2**  Open standard for Passwordless authentication  External key or platform key built in the device  No need for username and password  Latest standard – WebAuthn  FIDO2 is unphishable  Usually USB keys, Bluetooth or NFC  Sign in to Azure AD or Hybrid Azure AD joined win 10. SSO to cloud/onprem  Browser sign in  Enterprise with security sensitive, who don’t use phone for 2fa  Primary form of authenticaiton | **Microsoft auth app**  Sign in to any azure AD  Primary or secondary during sspr or azure ad mfa  Android / IOS |

MFA in Azure AD

Requires more than 1 form of verification

Something you know **and** something you have **OR** something you are

Forms of verification

1. Authenticator app
2. Hello for business
3. FIDO2
4. OATH software token
5. OATH HW token
6. SMS
7. Voice

Security Defaults – Comes with AZ AD free licensing

1. Enforces MFA registration for all users
2. Forces Admins to use MFA
3. Complete MFA authN when needed

Self Service Password Reset

1. Needs Azure AD licenses
2. Enabled for SSPR by admins
3. Registered with authentication methods. (2 recommended)

SSPR Authentication methods

1. App notification
2. Mobile Phone SMS
3. Office phone
4. Security questions (Not for admin accounts)
5. Email
6. App code

For admins to use SSPR – Usually Authenticator app, email address or phone number

Password Write Back – Write back to On Premise after password reset

Password Protection and Management Capabilities of Azure AD

Password Protection – Detects and blocks weak password

|  |  |  |  |
| --- | --- | --- | --- |
| Global Banned Password List | Custom Banned Password List | Protect against password spray | Hybrid Security |
| Managed by Azure AD IDP Team  Automatically applied and cannot be disabled | Brand Names, Product names,locations, internal company terms, abbreviations  Azure AD Premium 1 or 2 feature | Block weak passwords. | Hybrid on premise protection can be done  On premise receives global banned password list and custom password protection policy from azure Ad |

Graphical user interface, text, application

Description automatically generated

Azure AD Access Management Capabilities

|  |  |
| --- | --- |
| Conditional Access | Access Control |
| Implemented through policies  CA policy analyses signals like Users, Location, Devices, Application and Users Risks to decide authorizing | Block / Grant Access  Conditions  Microsoft defender for cloud apps – block download, cut copy, paste etc..  Labelling sensitive files.  Session control  Sign in frequency, app enforced restriction  Applied to groups or guests.  Paid Azure AD editions |

Azure AD Roles and RBAC

Azure AD supports custom and built in roles

Built in – Global admin, User admin, Billing admin

Permission in built in role cannot be modified

Custom roles - Create custom role definition and assign that role to users/groups by creating a role assignment

Scope – Resources role member has access to

Requires AZ AD P1 or P2

RBAC – Azure AD specific roles | Service Specific roles | Cross service roles

Azure AD RBAC - Azure AD roles control access to Azure AD resources such as users, groups, and applications.

Azure RBAC - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management.

Application

Description automatically generated

Describe Identity and Governance

Who needs access to what

What are they doing with that access

Any control for access management

Can controls be verified by auditing

Identity Governance – Identity Lifecycle

Azure AD Premium offers integration with cloud based HR system

Access Lifecycle – Managing access throughout the users org life

Dynamic groups – can be used

Privileged access lifecycle – Azure AD Privileged Identity Management PIM

Azure AD PIM – controls securing access rights

Azure AD, Azure and other MS Onl Svcs

PIM – Provides comprehensive set of governance controls

**Azure AD PIM – AD Premium P2**

**Entitlement Management – Premium P2**

Manage org. identity and access lifecycle at scale

Automates access request workflows, access assignments, reviews and expiration

2 Capabiliites – 1. Delegate the cration of access packages to non admins. 2. Managing B2B external users

**Azure AD access Reviews – Premium P2**

Effectively manage group membership

Access to enterprise apps and role assignment

Created from Azure Ad access reviews or PIM

Review and manage for both users and guests.

**PIM – Premium P2**

Manage, control and Monitor access to resources

Mitigates risk of excessive, misused, unnecessary permission

JIT – 0 to 24 hrs activation time

Time Bound assignment –

**Azure Identity Protection – Premium P2**

1. Automate the detection and Remediation of Identity based attacks
2. Investigate risk using data in the portal
3. Export risk detection data for 3rd party analysis

Sign In risk

1. Anonymous IP
2. Atypical travel
3. Malware linked IP
4. Unfamiliar sign in properties
5. Password spray
6. Azure AD threat intel

User Risks

1. Leaked credentials
2. Azure AD threat intel

3 Reports –

1. Risky users
2. Risky Sign ins
3. Risk detections

**MS compliance solutions**

Compliance.microsoft.com

Service Trust Portal – Information, tools and resources about MS Security, Privacy and Compliance practices

<https://servicetrust.microsoft.com/>

Compliance Manager – Microsoft PurView compliance. Microsoft 365

Trust Document – Audit Reports, Data Protection and Azure Stack

Industries and Regions

Trust center – Privacy, security and compliance in MS cloud

Resources – FAQ, security and compliance for O365. Microsoft Global DCs

My Library – Save documents. Notifications

**Microsoft Privacy Principles 6**

1. Control
2. Transparency – Informed decisions.
3. Security – Encryption. Protection in rest and in transit.
4. Strong legal protection –
5. No content based targeting – No sharing of data with advertisement services
6. Benefits to you – Data collection for Troubleshooting , Feature improvement and Personalized cust exp.

**Microsoft Privacy**

Priva Privacy Risk Management – Visibility into your organizations data and policy templates for reducing risk

* Monitor trends and activities
* Identify and investigate potential risks involving personal data
* Policy mgmt
* Subject rights request actions
* Setup policies identifying privacy risks
* Enable remediation
* Detect overexposed personal data
* Spot and limit personal data transfers

Priva Subject rights request – Automation and workflow tools for fulfilling data request.

* Data subject requests
* Data subject access requests
* Consumer rights requests
* Inquiries

Priva Scope

1. Exchange online
2. Sharepoint online
3. Onedrive for business
4. Teams

**Information protection and data lifecycle management in Microsoft Purview**

1. Classify
2. Protect
3. Retain data

Microsoft 365 Compliance is now called Microsoft Purview

Microsoft Information Protection - Microsoft Purview Information Protection

* Discovers, Classifies and protects sensitive content
* Tools to know your data, protect your data and prevent data loss

Microsoft Governance – Microsoft Purview Data Lifecycle Management

* Manages content lifecycle
* Import, store and classify data
* Govern own data

Know your data – Trainable classifiers, activity explorer and content explorer

Protect your data – Encryption, access restrictions and visual markings

Prevent data loss – Detect risky behavior, accidental oversharing. DLP, Endpoint DLP

Govern your data – Auto keep, delete and store data and records. Retention policies, retention labels and RM

**Data Classification**

3 Identification mechanisms – Manually by users, Automated pattern recognition, Machine learning

Sensitive Information Types – Pattern based classifiers

* Regex or function
* Credit card
* Passport or IDs
* Bank account numbers
* Health service numbers
* EDM – Exact Data Match – Custom sensitive information types

Trainable Classifiers

* Uses AI and ML
* Contracts, invoices or customer records
* Pretrained Classifiers – Ready to use
  + Resumes, Source code, harassment, profanity and threats
* Custom trainable classifiers
* Sharepoint online, exchange and onedrive

Classifiers only work with items that are not encrypted

**Content Explorer**

* Gain visibility into the content
* 2 Roles – Content explorer list viewer and Content explorer content viewer

**Activity Explorer**

* File copied to removable media, network share
* Label applied , changed

**Sensitivity Labels and Policies**

Sensitivity Labels - part of information protection

Labeling and protection of content

Applied to email and documents

Stamps are applied

Policies are applied based on the labels

Only 1 label at a time

Sensitivity labels can be configured to

* Encrypt
* Mark the content for office apps
* Apply the label automatically
* Protect content in sites and groups
* Extend to 3rd party via Microsoft Purview information protection SDK
* Classify content without any protection settings – Usage reports

use sensitive information types to identify specific types of information such as credit card number

Sensitivity labels are published to users and groups via label policies

Sensitivity labels help ensure that emails can only be decrypted only by users authorized by the label's encryption settings.

**DLP – Microsoft Purview DLP**

Detect Risky behavior and Prevent sensitive information shared

* Identify, Monitor and automatically protect
* Help user learn
* View DLP reports

**Endpoint data loss prevention – Windows 10, 11, macOS (Catalina and higher)**

Retention policies - Site level or Mailbox Level

Retention Labels – used to apply retention settings Item Level, Folder, Document or Email

Email/Doc – has only 1 retention lable 1 time

Default label – Sharepoint docs

**Records Management**

If a content is marked as regulatory record – not even global admin can remove label.

**Use Cases**

* Enabling manual apply retention and deletion actions for doc/email
* Auto apply retention and deletion actions
* Enabling site admins to default retain and delete - Sharepoint library, folder or doc set
* Enable users to auto apply retain/del actions to email – Outlook rules

**Insider risk management** is centered around the following principles:

Transparency: Balance user privacy versus organization risk with privacy-by-design architecture.

Configurable: Configurable policies based on industry, geographical, and business groups.

Integrated: Integrated workflow across Microsoft Purview solutions.

Actionable: Provides insights to enable user notifications, data investigations, and user investigations.

Escalating a case for investigation makes it possible to transfer data and management of the case to **eDiscovery (Premium) in Microsoft Purview.**

**Microsoft Purview Information Barriers** is supported in Microsoft Teams, SharePoint Online, and OneDrive for Business. information barriers only support two-way restrictions

**Office 365 core eDiscovery – Microsoft Purview eDiscovery (Standard)**

**Office 365 advanced eDiscovery – Microsoft Purview eDiscovery (Premium)**

eDiscovery – Identifying and delivering information

Search content in Exchange online, onedrive for B, Sharepoint Online, Teams, Groups, Yammer

Search mailbox and sites – export results

Identify, hold and export – from mbx and sites

eDiscovery (Premium) provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations.

User must be added to eDiscovery Manager role group – Purview compliance portal

eDiscovery (Premium) solution allows you to collect and copy data into review sets, where you can filter, search, and tag content so you can identify and focus on content that's most relevant.

The eDiscovery (Standard) lets you associate searches and exports with a case and lets you place an eDiscovery hold on content locations relevant to the case.

Audit (Premium) helps organizations to conduct forensic and compliance investigations by providing access to these crucial events.

**Auditing**

|  |  |
| --- | --- |
| **Standard** | **Premium** |
| 90 day retention  On by default  Org subscription + pre usr licensing | Longer retention  High value crucial event auditing  Bandwidth high  Org subscription + pre usr licensing |

|  |  |  |
| --- | --- | --- |
| **Azure Policy** | **Azure BluePrints** | **Microsoft Purview** |
| Enforce standards  Assess Compliance  Overall state of the environment  Per Resource, per policy level granular  Bulk remediation – existing resource  Automatic remediation – New resources  **Use case:**  Implementing governance for resource consistency  Regulatory compliance  Security  Cost and management  Evaluates all azure resources and Arc enabled resources  JSON format policy definitions  Policy initiative – Group multiple rules  Evaluation happens 24 hrs onces  Azure RBAC and Azure Policy should be used together to achieve full scope control | Define a repeatable set of azure resources  Rapidyly provision and run new envir.  In line with org. compliance  Provision azure resources across several subscriptions simultaneously  Declarative way to orchestrate  Role assignment  Policy assignment  ARM Templates  Resource groups  BP objects – replicated to multiple regions | Discover protect and govern sensitive data  Manage and govern on premise, muti cloud, SaaS data  Landscape of Org data,  Auto discovery, sensitive data classification and end to end data lineage  Data scanning and classification  Data Map – data discovery and govern  Data Catalog – find data  Data estate insights – Birds eye view |

**Security capabilities in Azure**

**DDoS – Azure DDoS Protection**

* Volumetric attacks – Flood nw with legitimate traffic. Measured in bits/sec
* Protocol attacks – Exhaust server resources with false protocol request

Exploit weekness in layer3 and layer 4

Measures in packets / second

* Resource application layer attacks – Targets web application packets.

Disrupt transmission or data b/w hosts

Azure DDoS – Basic and Standard

|  |  |
| --- | --- |
| Basic | Standard |
| Auto enabled for every property in azure  No extra cost  Always on traffic monitor  Real time mitigation of common network level attack | Extra mitigation capabilities  MI algorithms and dedicated traffic monitoring  Policies applied to public IP  Fixed monthly charge – protection 100 resources. |

Azure DDoS – Protects by analyzing traffic and take appropriate action on suspicious traffic

**Azure Firewall**

Protects Azure Virtual Network VNet

Can be done on any VNet but good to have on central VNet

Helps protect the Azure resources you have connected to Azure VNets

**Web Application Firewall**

Common exploit and vulnerability protection

Protects threats and intrusions

**Network Segmentation**

Isolation of resources , group related assets, governance

No traffic allowed across VNets or inbound to the VNet by default

Communication to be explicitly provisioned.

**Network Security Group -Protection within virtual networks**

Filter network traffic to and from Azure resources in Azure VNet

Only one NSG to each virtual network subnet

Only one NSG to each Network interface in a VM

NSG can be associated to many different subnets and network interfaces

**Inbound/Outbound Security Rules**

Azure creates 3 inbound/outbound default rules

Lower priority – Higher numbers

**Azure Bastion – PaaS**

RDP and SSH

No need public IP, agent or software or NSG

Port scanning protection

Azure bastion is deployed per Virtual network. Supports vnet peering

**JIT Just in time access**

Lock down of inbound traffic to your VMs

Microsoft Defender for Cloud – Threat protection and Security Posture Management – Deny all inbound

JIT needs Microsoft defender for servers to be enabled on the subscription

**Azure Encryption**

Azure Storage Service Encryption – Data at rest protection. Auto encryption

Azure Disk Encryption – Encrypt windows and linux IaaS vm disks. Bitlocker feature. DM-Crypt feature in linux

Volume encryption for os and data disk

Transparent Data encryption TDE – Protect Azure SQL DB and Azure Data warehouse. Realtime enc/decrypt of db, bkup, log

**Azure Key vault**

Central cloud service for storing app secrets.

Secrets Management – Store tokens, passwords, certs, API keys

Key Management – Create and control ecryption keys

Certificate mgmt – Provision, manage, deploy ssl certs for azure

HSM – Secrets protected by FIPS 140-2 level 2 validated HSM

**Cloud Security Posture Management CSPM – Tools**. Asseses and alert when vulnerability is found.

Continuously report and improve security posture.

**Microsoft Defender for Cloud** – Azure, Hybrid and other Cloud Platforms

* Continuously asses
* Secure
* Harden

MDC – Posture Management

* Visibility
* Hardening guidance

MDC – Cloud WorkLoad Protection CWP

* Detect and resolve threats to resources, workloads and services

MDC Free (For azure resources) & MDC with enhanced security features (For azure, hybrid and other cloud)

10 Defender Plans

* MD for servers – Threat det, and advanced defenses for windows and linux
* MD for App Service – Identifies attacks targeting applications over app service
* MD for Storage – Detects potentially harful activity on AZ storage accounts
* MD for SQL- Secures DB and data
* MD for Kubernetes – Cloud native Kubernetes security
* MD for container registries – Protect all ARM based registries
* MD for Key Vault – ATP for KV
* MD for Resource Manager – Monitors the resource mgmt ops in org
* MD for DNS – Azure DNS protection
* MD for Open source relations protections – Open source rdb protection

Enhanced Security Features

* Comprehensive Endpoint Detection and Response – EDR – MD for Servers
* Vuln scanning
* Multi cloud security
* Hybrid security – Univied view of security
* Threat protection alerts
* Track complainace – MD for Cloud
* Access and app controls – Block malware and other apps

Microsoft Sentinel – Alert detection, Threat visibility, Proactive hunting and threat response.

SIEM and SOAR

Intelligent Security analytics – Data is stored in Azure Monitor Log Analytics workspace.

Billing based on volume of data

**Capacity reservations and Pay as you go pricing**

Capacity reservation – fixed fee on the tier selected. Predictable cost

Pay as you go = Billed per GB

**Microsoft 365 Defender – Pre and Post breach enterprise defense**

Detection, Prevention, Investigation and Response across endpoints, identities, email and apps

Cross domain threat detection and response

Triage data

Self healing and automation

How threat occurred and what systems are affected. Automated action to prevent or stop attack

**Microsoft Defender for Identity + Azure AD Identity Protection** – Uses AD signals to id, detect and investigate

**MD for Endpoint** – Preventative protection, post breach detection, automated investigation and response

**Microsoft Defender for Cloud Apps** – Cross SaaS solution for cloud apps

**Microsoft Defender for Office 365** – Email messages, Links, and collaboration tools

|  |  |  |
| --- | --- | --- |
| MD for Office 365 | MD for Endpoint | MD for cloud apps |
| Email, links, teams, SP, Onedrive  Threat protection policy  Reports  Threat investigation and response  Auto investigation and response  2Plans   |  |  | | --- | --- | | Plan1 | Plan2 | | Safe attachment  Safe links  Attachment in office collab apps  Anti phishing  Real time detections | Plan 1 + Automation, investigation, remediation and simulation  AIR – Security playbooks  Attack simulator  Advanced hunting  Alerts and incident investigation |   MD for Office 365 – Microsoft 365 E5, Office 365 E5, Office 365 A5 and M365 Business Premium | Protect endpoints  Sensors – collect and process signal from OS, cloud security analytics, threat intel  Threat and Vuln mgmt  Attack surface detection  Next gen protection  Endpoint detection and response  AIR  Ms threat experts  Mgmt and API  Secure score for devices  Integrates with Intune and MD for cloud | Cross SaaS  Visibility into Shadow IT – cloud apps discovery  Cloud access security broker – casb  Broker realtime access b/w users and cloud resources  Office 365 cloud app security  Threat detection based on user activity logs, shadow it for apps, control permisisons to o365 and apply access and session control  Azure AD P1 – AZ AD cloud app discovery – Visibility into cloud app used |

MD for Identity – Uses On Premise AD Data (Signals)

* Monitor and profile user behavior and activities
  + Permission and group membership
  + Create behavioral baseline
  + Suspicious events and activites, insider threats
* Protect user Identities and reduce the attack surface
  + Defender for Identity security reports – helps id user and devices using clear text passwords
    - Extra insight on how to improve security posture and policy
  + If ADFS is present – Defender for ID protects by detecting on prem attacks.
* Identify suspicious activites and advanced attacks – cyberattack kill chain
  + Reconnaissance
  + Compromised credentials
  + Lateral movement
  + Domain dominance
* Investigate alerts and user activities

Portal.cloudappsecurity.com – Defender for cloud apps

Defender portal

Hunting – Query based hunting – 30 days of raw data

MDefender for cloud – Security posture for Azure subscription

M365 Defender portal – Security posture of organization across your apps

Compliance covers data residency and regulatory compliance.

Through the Data Security pillar, an admin can identify and control sensitive information and respond to classification labels on content

SC 900 CRAM

**Defense in depth**

Data – Encryption at rest, Encryption at transit

Application protection

Compute protection

Network – Segmenting, NSG

Perimeter Protection – DdoS

Identity – MFA

Physical Security

Confidentiality – Encryption

Integrity – Not tampered with

Availability – Available to those who needs it

**Security**

Threats – **Identity thefts**

Data breach, Dictionary attacks (**Azure AD Smart Lockouts** can protect ad account)

Phishing – Email coming to users

Spearfishing - focused attack. Like email from manager

**Availability / Disruptive attacks**

Ransomware – Encrypt data

DDoS – Service attack

**Zero Trust**

Assume compromise

Trust nothing and Verify Everything

Authentication + Authorization

Least privilege – Just in Time (Get permission only when required)

Just enough administration – Just enough privilege

Assume breach – Segment everywhere in the network, Encrypt, Detect threats

**Focus on**

Identity

Device monitoring

Applications

Data classifications – Encrypt + DLP

Infrastructure protection

**Encryption Types – 2 types**

Symmetric Encryption - Uses same key

Asymmetric Encryption – Uses public and private key pairs

Integrity – Making sure no one messed with data.

Hashing does integrity

Data encrypted with private key -> Send to person with hash value

Person gets data and runs hash algorithm and decrypt the hash value with public key and sees if the hash matches

**6 Key Privacy Principles**

1. Control – putting customer in control
2. Transparent – what is collected etc..
3. Security –
4. Strong legal protection – respecting local laws, rights
5. No Content based target – no personal content advertising
6. Benefits to you – collecting data and using6.

**Trust**

Service Trust Portal – servicetrust.microsoft.com

Documents, reports, whitepapers, Audit reports, compliance manager

Compliance manager – improvements and management

STP – library to save documents

**Azure AD**

1.Azure

2.Microsoft365

|  |  |
| --- | --- |
| Azure | M365 |
| Administration  Modern Authentication  Token  Consenting  Policy  Audit  Risk  Authentication  Authorization  Audit |  |

AAD Cloud is the new name

AAD Connect – Sync, seamless

Azure AD –

Users, Groups, Guests ( B2B – different AD, MS Account, outside people)

Service Principle – application registration

Managed identity – Resource getting identity

Groups – 1. Assigned (Manually) 2. Dynamic (Query)

Group – assign licenses or roles

Devices – 1. Joined – authenticate with Azure AD

2. Registered – Personal devices (ios, wind10, macos, android)

3. Hybrid – both azure AD and On prem AD connected

Separate tenant B2C - Customers – Azure AD Business to Customers

FB, Twitter – can authenticate to Azure AD

Azure AD Pricing

M365 licenses free

Premium AD – conditional access,

P2 – PIM, id protection, JIT, etc..

No Password authentication – TPM on laptop (creates private public key), Hello 4 Business

MFA Fraud alert – not initiated 2fa request

Per User MFA and Conditional Access **(p1 or p2 license)**

CA – policies and do MFA

M365 – **Per user MFA**

SSPR – Change, reset unlock accounts

Block simple password

Authorization –

RBAC

Azure AD & M365

Conditional Access

Terms of use – make them accept

Location – Public IP, geo location

Policy

Session control – something like no save only read, login in intervals etc.

**Auditing & governance**

[P2] Azure Ad doesn’t have governance natively

[P2] Dynamic Group based on user attributes

[P2] Privileged Identity Management

[P2] Access reviews (App, role, group)

[P2] Azure AD ID protection

Root of azure is

azure AD tenant –

Root Management group –

Management Groups –

Subscription –

Resource Groups –

Resources – (Locking - Cannotdelete, Read Only) These are in management plane. Not in Data plane.

RBAC, Policy , Budgets

ARM Template – Declarative, JSON

Blue print - Deploy resources in standard way . Define RG, RBAC, Policy and ARM templates

Blue print – Collection of things, standard set of configs

Guard Rails - Policy. Only use these region, this tags, this resource

Cloud Adoption Framework – Set of documents and guidelines of Best practice.

Strategy, planning, ready, adopt, migration, innovation etc..

Network and Data and Virtual Network

VNET - > NSG – IP + Port + Protocol

Allow / deny rules

ASG – Has tag on the network interface or IP

Public IP address – DdoS – Basic and Standard (Traffic monitoring, machine learning, custom policies)

Azure firewall – Appliance in virtual network. Native HA. Filter on IP, FQDN. Outbound SNAT

Web application firewall – exploit protection

Azure Bastion – From Azure portal – connect via Bastion – RDP/SSH connection to Virtual networks

**Storage Accounts –**

Encryption at rest –

Platform Managed Key – Microsoft manages, stores/rotates

Customer Managed Key – Key vault

VM – Azure Disk Encryption

Key vault –

Certs , Secrets – data , keys to perform crypto operations (cant be retrieved)

**Azure Security Center**

Secure score, Regulatory compliance, Recommendations, Azure defender

Tells the compliance state, protection

**Azure Sentinel**

Log analytics work space.

Has connectors. Connectors to Azure AD, M365 etc

Adds machine learning to give analysis. SIEM + SOAR

**M365 – Defender**

Defender for Identity – Looks on premise for security

Defender for endpoint – anti malware. Forensic analysis. Win, android, linux, macos

Cloud app security – What application from corporation speaks to azure, byod, discovery, Conditional access and proxy control

* Data exfilteration control

Defender for Office365 –

Office 365 Defence of Depth – Identity, Device, Data

Security Center – Secure score, Reporting, incident

**Device Security** –

Intune – policy, health (Macos, windows, android,ios) , app push custom as well

MDM – Mobile device management – enrolling device

MAM – Mobile App Management – App policies

**Security baseline for windows 10 devices**

**Data – Classify and Protect**

**Ediscovery – Find and Action**

Content search

Core ediscovery – Case, search, hold, export

Advanced ediscovery - all above + process data, add custodians etc..

**Hold will take 24 hrs**

**Compliance Solutions**

**Insider risk management** – Alert + Triage – Notification. Helping detect and prevent insider actions

**Communication compliance** –

**Information Barrier** – Users shouldn’t communicate with each other via teams sharepoint and onedrives

**PAM** – Task and scope.

**Customer lockbox –** Access to data by customer support

Microsoft Defender for Endpoint -= Microsoft ATP

**Compliance.microsoft.com**

Compliance Manager – Measures opportunity to protect data and comply with standards and regulations

Classifiers – Identify, protect and govern sensitive data.

Microsoft Purview – Compliance portal

Compliance Score – Reduce risk around data protection and regulations

Defender for Endpoint – Security Platform.

Helps prevent, detect, investigate and respond to advanced threats.

**Modern authentication**

Center is Identity Provider

Supports SSO

**Azure Active Directory**

Employee, guest and others

4 types of identiies - Users, service principal, managed identity, device

Text

Description automatically generated

External Identities

B2B – Share your apps and resources with external users

B2C –

MFA – Phone, MS Auth, OAuth.

Password less – Biometrics, Microsoft Auth, FIDO2

Reset password – 1 or 2

Global banned password list

Custom banned password list

Protecting against password spray

Hybrid security

Conditional Access – AD Premium feature

Graphical user interface, application

Description automatically generated with medium confidence

**RBAC -**

Built in Roles

Custom Roles

Azure AD RBAC

Only grant the access users need

**Identity Protection and governance capabilities**

Entitlement Management –

Manage identity and access lifecycle at scale

Automates access request, workflows, access assignments, reviews and expiration

Create access packages. User can go and request that package to get access

Expiration policies can be set

**PIM – Privileged Identity Management**

Just In Time. Access only when needed and how much needed

Time bound – start and end dates

Approval based

Notifications

Auditable

Text, letter

Description automatically generated

**Azure Security**

**NSG**

Limit what type of traffic in / out vNet – **Network security group**

**NSG** Rule properties – Name, Source, Dest, Direction, Action, Priority, Protocol, Port Range

Multiple subnets / security groups association

Cannot delete default rules but can override using priority

Network interface to be associated with NSG

**Azure DDoS Protection** – Analyze network traffic and discards DDoS

Basic + Standard

Azure has built in DDoS protection – basic

Standard – extra monitoring and mitigation tools

**Azure Firewall** – Protect perimeter

Graphical user interface, text, application

Description automatically generated

Azure Bastion

Graphical user interface, text

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

**Azure Encryption – Data at Rest**

**Graphical user interface, application, website

Description automatically generated**

TDE – SQL DB and Data warehouse, backups and logs

Organizational secrets – Central place for all app secrets

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Policy – Default allow / deny – Resources based

Blueprint – policy can be included in blueprint.

**Azure management tools for security**

**CSPM**

Central security management

**Graphical user interface

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**Security center -**  shows multiple subscriptions

**Azure Defender**

Graphical user interface, application

Description automatically generated

Table

Description automatically generated

**Azure Sentinel** – Collect, Detect, Investigate and Response

**Graphical user interface

Description automatically generated with medium confidence**

SIEM – collect data, alert

SOAR – Gather alert and trigger workflow

XDR – Automated response

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generatedTable

Description automatically generated with medium confidenceGraphical user interface, application, email

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

A picture containing graphical user interface

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedTable

Description automatically generated with medium confidenceTable

Description automatically generatedTable

Description automatically generatedTable

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedTable

Description automatically generated