# 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

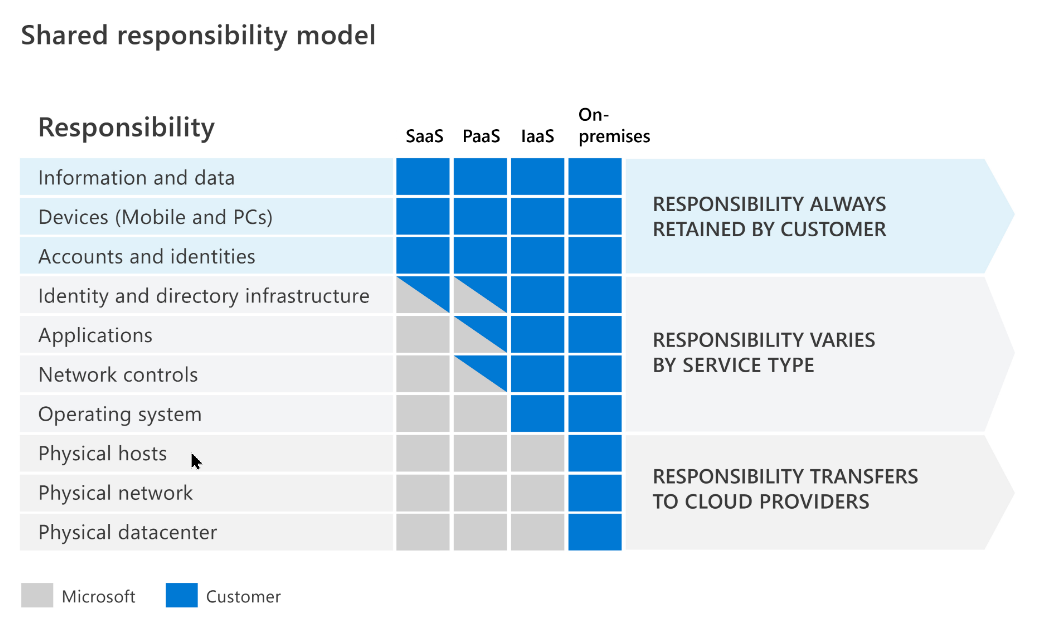
Spoofing wifi hotspots – free wifi attack

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**

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

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