Azure security features

Azure security centre

* Monitoring service that provides visilbility of security posture. It can:
  + Monitor and apply security settings
  + Provide security recommendations
  + Use ML to block malware from VMs
  + Detect inbound attacks
  + Provide just in time access control for network ports
  + Provide analysis against frameworks such as PCI DSS/CIS

* **Secure score:** Measurement of organisational security score
* Security centre capabilities:
  + Just in time VM access
  + Adaptive application controls: Control which apps are allowed to run on VMs
  + Adaptive network hardening: Monitor internet traffic patterns of VMs and compare it with the current network security group settings.
  + File integrity monitoring

Azure sentinel

* SIEM which allows you to:
  + Collect cloud data at scale
  + Detect threats
  + Investigate threats with AI
  + Respond to incidents rapidly

* Search for activity across environments via either built in analytics or custom analytics for specific criteria
* Azure monitor workbooks can be used to automate threat responses, such as automatically alerting for specific Ips

Azure key vault

* Stores an application's secrets in a central location, and uses access control and logging to keep it safe
* It can:
  + Manage secrets
  + Manage encryption keys
  + Manage TLS/SSL certs
  + Store secrets backed by hardware security modules (HSM)
* Benefits:
  + Centralised app secrets, allows you to control and monitor distribution
  + Securely store secrets and keys
  + Access monitoring and access control
  + Simplified key administration
  + Integrate with other services

Azure dedicated host

* Provides dedicated physical servers to host VMs - good for compliance requirements where they should be the only customer hosting a VM on that physical machine
* A dedicated host group is a group of dedicated hosts. This can be used to enhance availability

* Benefits:
  + Full visibility and control over server infrastructure
  + Address compliance requirements
  + More control over number of processors, capabilities, and VM size
* Customers are charged per dedicated host, regardless of how many VMs are deployed on it.

Securing network connectivity

* **Defense in depth:**
  + Physical layer: Controlling access to hardware and datacenters
  + Identity and access layer: SSO and MFA, auditing
  + Perimeter layer: DDoS protection and perimeter firewalls
  + Network layer: Deny by default and restrict inbound access. Secure connectivity between resources
  + Compute layer - access to virtual machines and endpoint protection
  + Application layer - software vulns, app secrets, and security by design
  + Data layer: controlling access to data

* **Azure firewall** - PERIMETER LAYER
  + A stateful firewall that uses a static public IP addr, integrated with azure monitor
  + Benefits:
    - High availability
    - Cloud scalability
    - Inbound and outbound filtering
    - DNAT support
  + You deploy this on a central virtual network

* **DDoS protection** - PERIMETER LAYER
  + Uses scale and elasticity of the microsoft global network to bring DDoS mitigation capacity to every azure region. It blocks attacker traffic and makes sure that you only pay for valid customer traffic.
  + It can protect against volumetric attacks: which flood the network layer with seemingly legitimate traffic, protocol attacks: render a target inaccessible by exploiting a weakness in the layer 3 and layer 4 protocol stack, and Resource-layer (application-layer): target web application packets to disrupt the transmission of data between hosts. WAF is needed here.
  + Service tiers:
    - Basic: Always-on traffic monitoring and real-time mitigation - automatically enabled
    - Standard: Additional mitigation capabilities that are tuned specifically to Azure Virtual Network resources. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms.

* **Network security groups:** NETWORK LAYER
  + Internal firewall for virtual networks providing ingress and egress filtering to and from azure resources
* **Azure application gateway:** 
  + Has WAF for web apps