Defense in Depth (concentric layers diagram)

Physical
Identity & Access
Perimeter
Network
Compute
Application
Data
Memory

MY BADGE, Background Checks

Virtual Network

NSG,
Azure Firewall,
DDOS
Routing Tables,
Service Endpoints,
Private Endpoints,
Application Gateway
Azure Front Door
Traffic Manager
Bastion

Azure Active Directory

SSO, Multi-factor
Authentication,
Password reset,
Azure AD Groups,
Service Principals,
Managed Identities

Azure Subscription

RBAC
Azure Blueprints
Azure Policy

Virtual Machines
VM Patching,
VM Extensions:
Malware, DSC – Desired
State Configuration,
Disk Encryption
Just-In-Time Access

Application Level

Azure Key Vault
Access Policies
Authorization Attributes
CORS (Cross-Origin Resource Sharing)
DevSecOps
API Management Policies

Trusted Secure Environments

Data in use
Confidential Computing

Data

Access Keys
Container Access Levels
SAS Tokens
Encryption At Rest
Encryption in Motion
Row-level Security
Advanced Threat Detection
Transparent Data Encryption
Dynamic data masking

Subnet Connected Defense in Depth

PaaS Services & Virtual Machines — VM Firewall — VM or NIC NSG — Subnet NSG — Virtual Appliances — Load Balancer — DDoS Protection — Internet

Defense in Depth in securing ICS

Plan for Security (Responsibility table)

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Customer	Customer	Customer	Customer
Client & end-point protection	Customer	Customer	Customer	Customer/Provider
Identity & access management	Customer	Customer	Customer/Provider	Customer/Provider
Application level controls	Customer	Customer	Customer/Provider	Provider
Network controls	Customer	Customer/Provider	Provider	Provider
Host infrastructure	Customer	Customer/Provider	Provider	Provider
Physical security	Customer	Provider	Provider	Provider

Cloud Customer / Cloud Provider

Plan for Security

Azure OMS	Azure Security Center	Azure Monitor
Azure Network Watcher	Azure Storage Analytics	Azure Active Directory

Options for System Protection
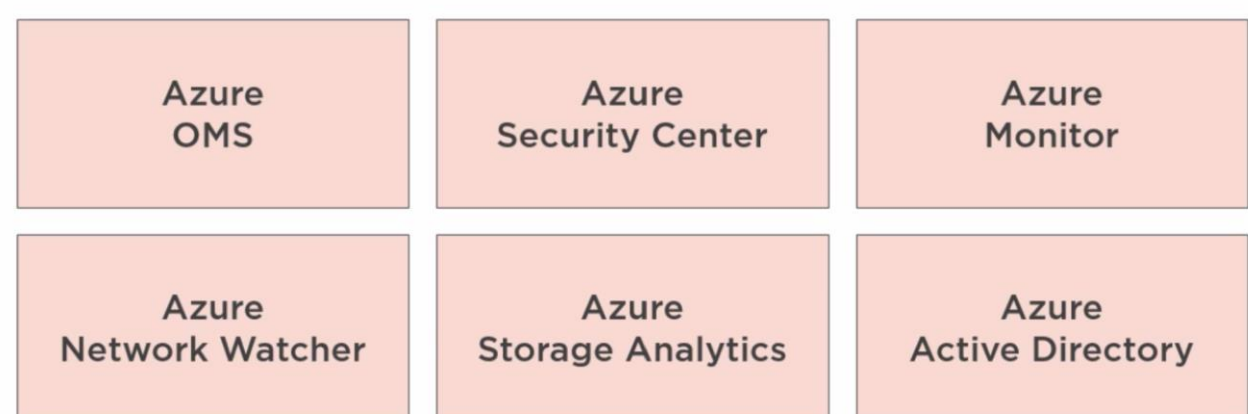
Application/service replication
Application/service DR solution
In-OS replication
Storage replication
Hypervisor replication
Recreation of stateless services from template
Backup restoration

Pillar	Description
Scalability	A system's ability to handle increased load.
Availability	The proportion of time that a system is functional and working.
Resilience	A system's ability to recover from failures and continue to function.
Management	Operations processes which keep a system running in production.
Security	To protect applications and data from threats.