convergent

Azure Remote Production Deployment and Hardening Guide v1.0

20th July 2022

PUBLIC RELEASE

Disclaimer

The information contained in this guide is based upon a collection of methodologies, policies, and procedures at a single point in time and intended for use by Microsoft Azure Customers for the purposes of securely deploying a remote-production architecture on Azure cloud platform. This guide is provided for informational purposes only and is provided “as is.” Convergent cannot guarantee the accuracy of any information presented after the date of publication. Except as set forth in Convergent’s terms and conditions and/or any other agreement you sign with Convergent, Convergent assumes no liability of any nature in relation to how this information is used by the recipient.

Document Control

Version	Date	Name	Action
0.1	24th Jan 2022	Nipun Mehta	Author
0.2	26th Jan 2022	Convergent Team	QA
0.3	26th Jan 2022	Nipun Mehta	1st Draft Release
0.5	27th April 2022	Nipun Mehta	Updates
0.6	19th July 2022	Nipun Mehta	Updates
0.7	20th July 2022	Convergent Team	QA
1.0	20th July 2022	Nipun Mehta	**Final version released**

Table of Contents

Figures and Tables

1. Executive Summary

Microsoft has engaged Convergent Risks to review remote production architectures and workflows leveraging the Microsoft Azure Cloud platform with the purpose of providing Azure specific deployment and hardening guidance for the Media and Entertainment (M&E) industry.

The Microsoft Azure platform can be leveraged to manage, transform, and deliver media content with cloud-based workflows. The Azure media services can help the M&E industry to build media applications using low-latency live streaming, batch encoding, content protection (DRM) and deliver streaming content to millions of viewers on any device anywhere in the world. The purpose of this document is to provide vendors and content owners with clear and concise guidance on Azure media services deployment, cloud native, and Microsoft offered security controls that can be leveraged from the Azure Cloud platform.

Recommended deployment best practices and guidance is based on analysis of existing Microsoft documentation and reference architectures, architecture review and mapping of industry best practice recommendations and compliance standards (e.g., Zero Trust Architecture, CSA CAIQ, CIS, MPA etc.). This document is current as of July 2022. Any changes to Azure services after this date should be verified via Azure portal to ensure any applicable updates are considered.

2. Introduction

Microsoft Azure is Microsoft's public cloud platform that offers cloud computing services for building, testing, deploying, and managing applications and services through Microsoft's data centers around the world. Azure provides Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services to its customer base along with support for various application languages, tools, frameworks and integration with third-party products and services.

Azure Media Services is a PaaS offering for encoding, content protection, streaming and analytics. Some of the key concepts for Azure media services include assets and storage, jobs, and tasks, encoding, live streaming, protecting content and delivery. Recent change in the ideology of on-premises operations has given boost to different creative ideas of remote working in various sectors, and whereas not completely new, an increased focus has supported remote production capabilities in the M&E industry.

Remote production also known as "at-home" production or Remote Integration (REMI) is a workflow wherein live event content is captured and sent over IP links to a centralized production facility where the final program is produced and distributed. Remote production in cloud involves encoded Serial Digital Interface (SDI) feeds streamed to the cloud-based SaaS platforms. Some of the advantages of remote production in cloud include fewer staff and equipment requirement onsite, lowering travel expenses and logistical costs. The studio is also able to cover multiple events in a single day with the same personnel.

Regardless of whether it is content creation, live streaming of events and shows or streaming OTT platforms, the cost and resource challenges are applicable to all these workflows. Typically, the costs for different workflows within these areas are made up of multiple elements including logistics, staffing, facility, talent, production, and content distribution. Recent changes in ways of working due to the pandemic has made it a key business requirement for the majority of these workflows to be developed and ran remotely which not only provides resources with remote capabilities but also the required flexibility for the content creators. By using microservices, infrastructure on demand and creating flexible pipelines using various SaaS based solutions in cloud, a lot of cost and flexibility challenges can be mitigated.

Security is a key focus of this deployment and hardening guide hence subsequent sections go in more detail covering recommended best practices from various sources including the Azure Cloud Adoption Framework (CAF) Security Best Practices, Azure Security Best Practices, Azure Security Baseline for Services, and Convergent's Cloud Security Best Practices. Additionally, Azure Security Best Practices have been further mapped to relevant frameworks and standards applicable to the media and entertainment industry. Figure 1 – Azure Security Controls Suite below gives an overview of the various security controls and practices reviewed for this guide, and how the respective set is applicable depending on your requirements.

Whereas there will be some overlap between all the security controls and practices mentioned below, their applicability and when they should be used will depend on what stage of the cloud journey your organization is at and your overall purpose of using this guide.

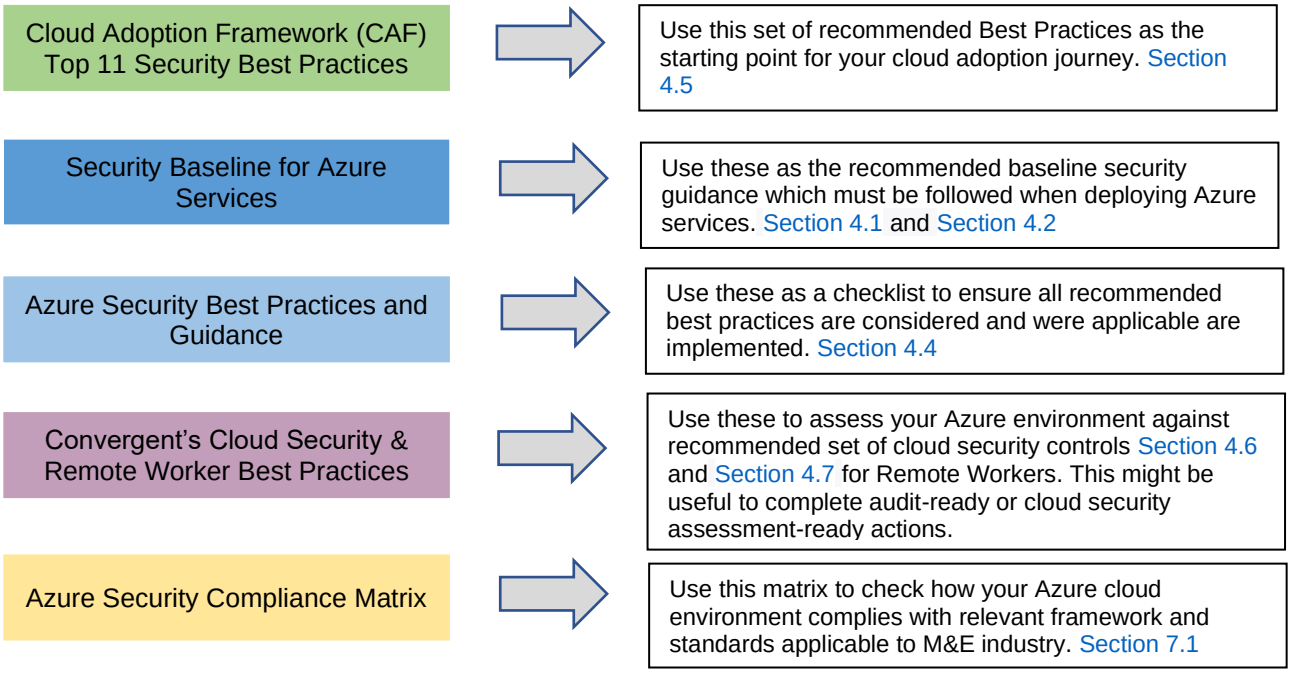

Figure 1- Azure Security Controls Suite

3. Remote Production Architecture

The concept of Remote Production or Virtual Production has clearly got more demand for it in present times than ever before. Workforce is adopting remote working environments and the ability for artists and technicians to be able to support different workflows and complete pre and postproduction activities from anywhere in the world is now a key business requirement. With the use of cloud platforms like Azure, the traditional challenges of latency and global availability can be now mitigated. Technologies like Extended Reality (ER), Remote Rendering, Camera to Cloud and Live Streaming to cloud can all be used by leveraging cloud-based services to integrate with them and provide ability to scale services on-demand and hence providing with more instant feedback loop for the content creators as part of the workflow. Using cloud-based services content creators can now have production ready environments created within minutes to hours saving on cost and efficiency. Whereas there are a lot of benefits with these architectures, it is important to understand the dependencies and security requirements before defining and deploying these systems.

3.1 Remote Production – Live Streaming

Live streaming could be used for variety of media broadcast like sports, concerts, news etc. Typically, these broadcasts are managed via a production control room wherein the incoming feeds are combined, and the outgoing program is created. With introduction of cloud platforms, these control rooms could be virtualized in cloud which could add benefits like dynamic on-demand scaling of resources (avoiding costs on expensive hardware), enabling remote working capabilities hence ensuring that workforce can contribute from anywhere in the world and improved productivity as you can manage multiple events from the virtual control room (saving time on travel between venues).

Azure Media Services (AMS) is a cloud-based PaaS service that enables users to build solutions that achieve broadcast-quality video streaming. Some of the common use cases for leveraging AMS includes:

- Deliver videos in various formats which can be played on variety of browsers and devices
- Streaming live events to large audience online
- Analyze recorded videos our audio content
- Create a subscription video service and stream DRM protected content when a customer (for example, a movie studio) needs to restrict the access and use of proprietary copyrighted work
- Deliver offline content for playback on airplanes, trains, and automobiles
- Use Azure Media Services together with Azure Cognitive Services APIs to add subtitles and captions to videos to cater to a broader audience

To stream live events with Azure Media Services, following key components are required:

- A camera to capture the live event or use tools such Telestream Wirecast to generate live feed from a video file
- A live video encoder that converts signals from a camera (or another device, like a laptop) into a contribution feed that is sent to Media Services
- Components in Media Services, which enable you to ingest, preview, package, record, encrypt, and broadcast the live event to your customers, or to a CDN for further distribution

A live event can be set to either a pass-through (an on-premises live encoder sends a multiple bitrate stream) or live encoding (an on-premises live encoder sends a single bitrate stream). In the pass-through Live Event (basic or standard), the on-premises live encoder to generates a multiple bitrate video stream and send that as the contribution feed to the Live Event (using RTMP or fragmented-MP4 input protocol). The Live Event then carries through the incoming video streams to the dynamic packager (Streaming Endpoint) without any further transcoding (See Figure 2 - Pass-through). Such a pass-through Live Event is optimized for long-running live events or 24 x 365 linear live streaming.

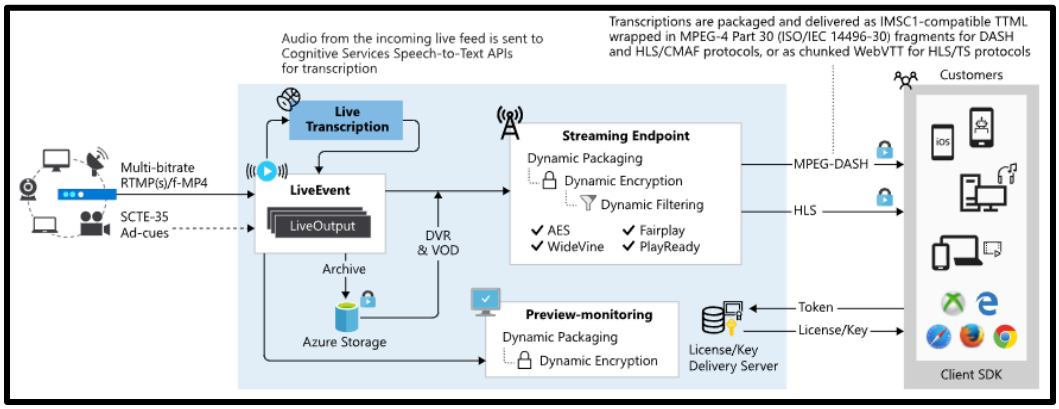

Figure 2 - Pass-through[1]

When using cloud encoding with Media Services, on-premises live encoder is configured to send a single bitrate video as the contribution feed (up to 32Mbps aggregate) to the Live Event (using RTMP or fragmented-MP4 input protocol). The Live Event transcodes the incoming single bitrate stream into multiple bitrate video streams at varying resolutions to improve delivery and makes it available for delivery to playback devices via industry standard protocols like MPEG-DASH, Apple HTTP Live Streaming (HLS), and Microsoft Smooth Streaming (see Figure 3 – Live Encoding).

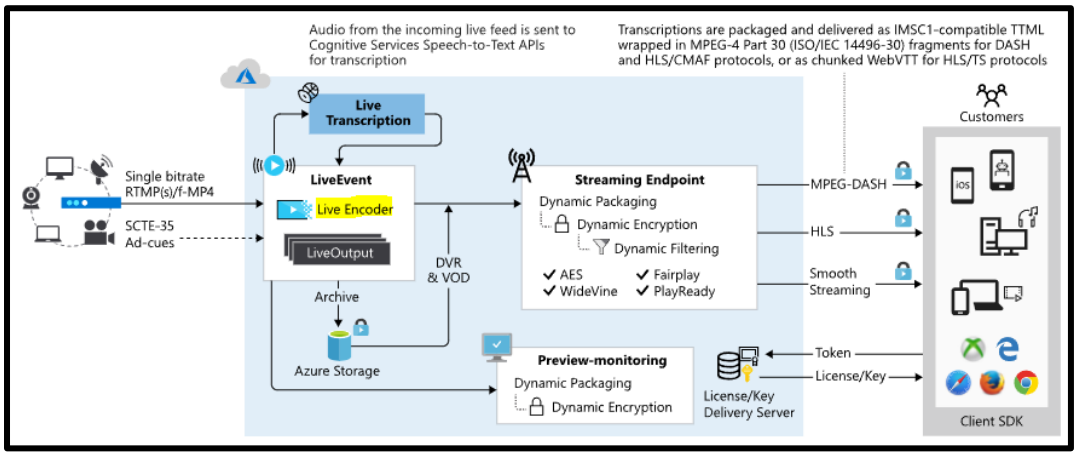

Figure 3 - Live Encoding[1]

[1] https://customers.microsoft.com/en-us/story/haivision-media-telecommunications-azure

3.2 Remote Production – Content Creation

There are various SaaS solutions that can be leveraged to support remote production requirements in cloud. One such platform is Grass Valley's GV AMPP (Agile Media Processing Platform). GV AMPP is specifically designed to overcome broadcasters' long-time reliance on costly and inflexible hardware-based media systems. Different media workflows run on the variety of modules available on the AMPP platform which leverages various microservices in the cloud. This approach ensures that the customer is only charged for the services used hence making it a cost-effective solution. It can run in any data center or public cloud environment like Azure.

Haivision's SRTHub is a blended PaaS/SaaS solution that optimizes broadcast-quality video across the globe. It uses Microsoft Azure Container Services as the key underlying technology to provide this solution on demand. Whereas use of SRT addresses many of the latency and reliability issues, leveraging Azure platform helps to overcome global availability and fast, low-overhead deployments. Use of containers ensures that SRT sender and receiver services can be spun up and down on demand within Azure. Some of the other Azure services leveraged by SRTHub include - Azure Cosmos DB as the globally distributed, multi-model database, Azure Functions for access to APIs, Azure Key vault for encryption and monitoring, Azure Container Registry to deploy container images and Azure Blob storage to store them, Azure IoT Hub, and Azure IoT Edge services to provide remote controls and management for SRTHub connected applications, workflows and encoding services. Figure 4 – SRTHub via Azure below gives a high-level overview of the solution.

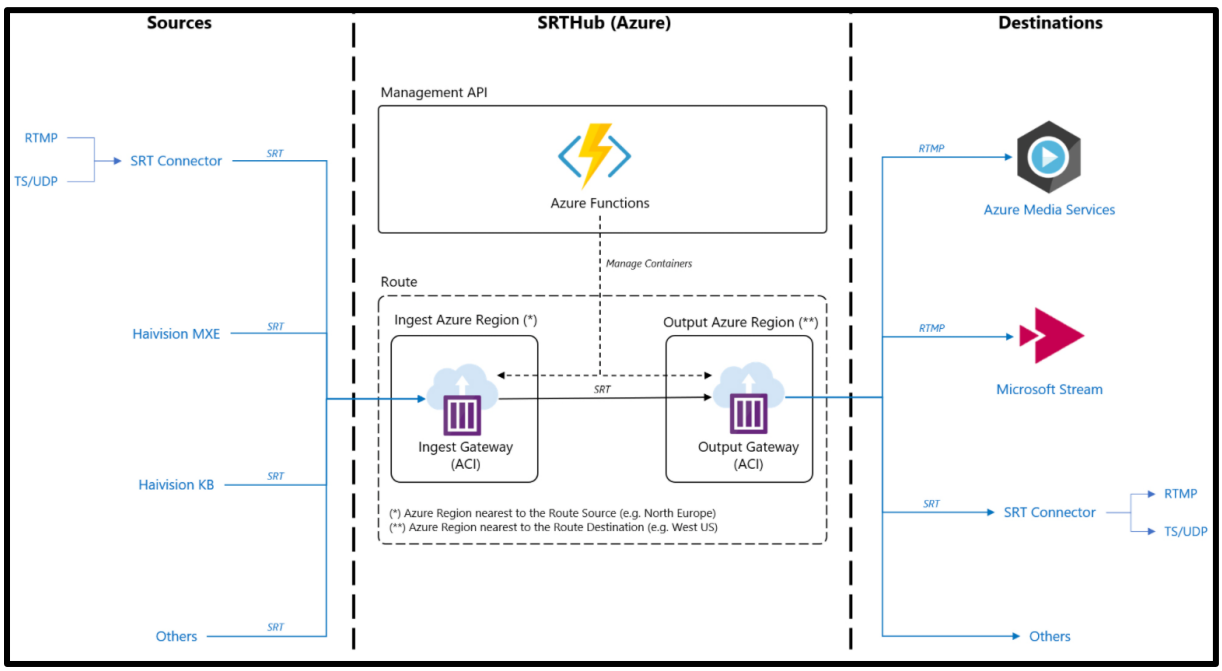

Figure 4 - SRTHub via Azure[2]

[2] https://customers.microsoft.com/en-us/story/haivision-media-telecommunications-azure

3.3 Remote Production – Camera to Cloud (C2C)

In video production, Camera to Cloud (C2C) is workflow that enables filmmakers to export original footage into a post environment as soon as it is recorded. Video content can be reviewed, edited, and sent back to the set hence saving time, money and enhancing creative decision making. This workflow can also be used for remote production live streaming.

Azure Video Analyzer service allows users to connect Real Time Streaming Protocol (RTSP) cameras directly to the cloud to capture and record video using live pipelines. These pipelines allow you to ingest, process and publish videos within Azure cloud environment. Azure Video Analyzer currently supports three different methods for connecting cameras to the cloud (see Figure 5 below):

- **Connecting via a remote device adapter** – the edge module acts as a transparent gateway for video traffic between the RTSP cameras and Video Analyzer service. This can be useful when camera devices need to be protected from direct internet access, when camera devices cannot connect to IoT Hub independently or when on-premises facilities limitations only permit lightweight edge device. Additional details can be found by following this how-to guide
- **Connecting from behind a firewall using an IoT PnP command** – using the IoT Plug and Pay command interface, the camera devices connect directly to Video Analyzer behind a firewall. This option requires an IoT PnP device installed and run on camera devices. Additional details can be found by following this how-to guide
- **Connecting over the internet without a firewall** – it is recommended that this method is only used for supervised proof-of-concept where it is permissible to allow Video Analyzer service to access the device over the internet without a firewall.

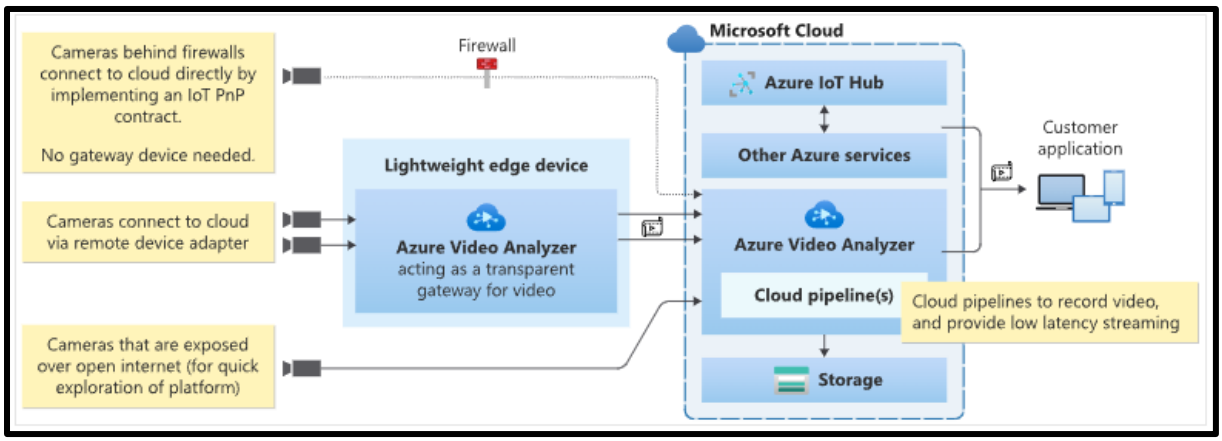

Figure 5 - C2C using Azure Video Analyzer[3]

[3] https://docs.microsoft.com/en-us/azure/azure-video-analyzer/video-analyzer-docs/cloud/connect-cameras-to-cloud

3.4 Remote Production – Extended Reality (XR)

Extended Reality (ER) is an umbrella term that covers Augmented Reality (AR), Mixed Reality (MR), Virtually Reality (VR) and any other variations. VR is typically described as a 3D computer generated environment which can be explored and integrated with by the end user. Within this environment, the end user is immersed in the environment and able to manipulate objects or perform series of actions. Augmented Reality (AR) does not give a complete immersion rather it adds digital elements to a live view. Mixed Reality (MR) is a combination of key elements from both AR and VR where physical and digital objects coexist and interact in real time.

Within the media and entertainment industry, AR has been used for example to engage audiences and promote new releases as a marketing strategy and VR has been leveraged by Disney Movies VR which provides a range of immersive experiences for Disney fans e.g., exploring favorite Disney scenes in more detail. Different game engines that have been traditionally used for games development can also be leveraged along with virtual production for content creation. Unity and Unreal are two of the most commonly used game engines. Using these game engines enhances collaboration at every stage of the workflow and helps to shorten the feedback loops. As a scene is being shot, teams can track its progress and the creative team of writers, directors, editors, artists etc. can decide on the final shots and more importantly this can be all achieved in real time.

For the game engines and virtual production to work together key elements such as Project Management (e.g., Agile) and Asset Tracking and Data Management (to manage and store large files and massive number of iterations) are required. Cloud platforms like Azure can be leveraged to deploy systems to maintain high availability across regions and to secure assets. To create content using game engine like Unity in a virtual production environment it is important to build a pipeline that optimizes the overall workflow. Key elements like management of remote contributors, large files, different types of digital assets, numerous iterations and security for the valuable IP are important considerations when building a pipeline. Helix Core version control from Perforce can be useful to store all virtual production and unity assets and manage multiple iterations over time. Helix Core can be deployed in Azure and can integrate with commonly used tools like 3ds Max, Maya etc.

Perforce also offers Enhanced Studio Pack (ESP) via Azure Marketplace which helps to build a pre-configured production ready environment in cloud. The ESP turn-key bundle includes:

- Helix Core – Version Control
- Helix Swarm – Code Review
- Hansoft – Project Management
- Windows Workstation – Virtualized Desktop with GPU
- Infrastructure as Code (IaC) and configuration management with smart defaults built in

ESP uses Server Deployment Package (SDP) to deploy Helix Core product onto the Linux CentOS 7.9 server. It provides a highly resilient production-ready environment with high availability. Figure 6 – Perforce ESP on Azure illustrates a high-level topology that gets deployed in Azure using the ESP bundle.

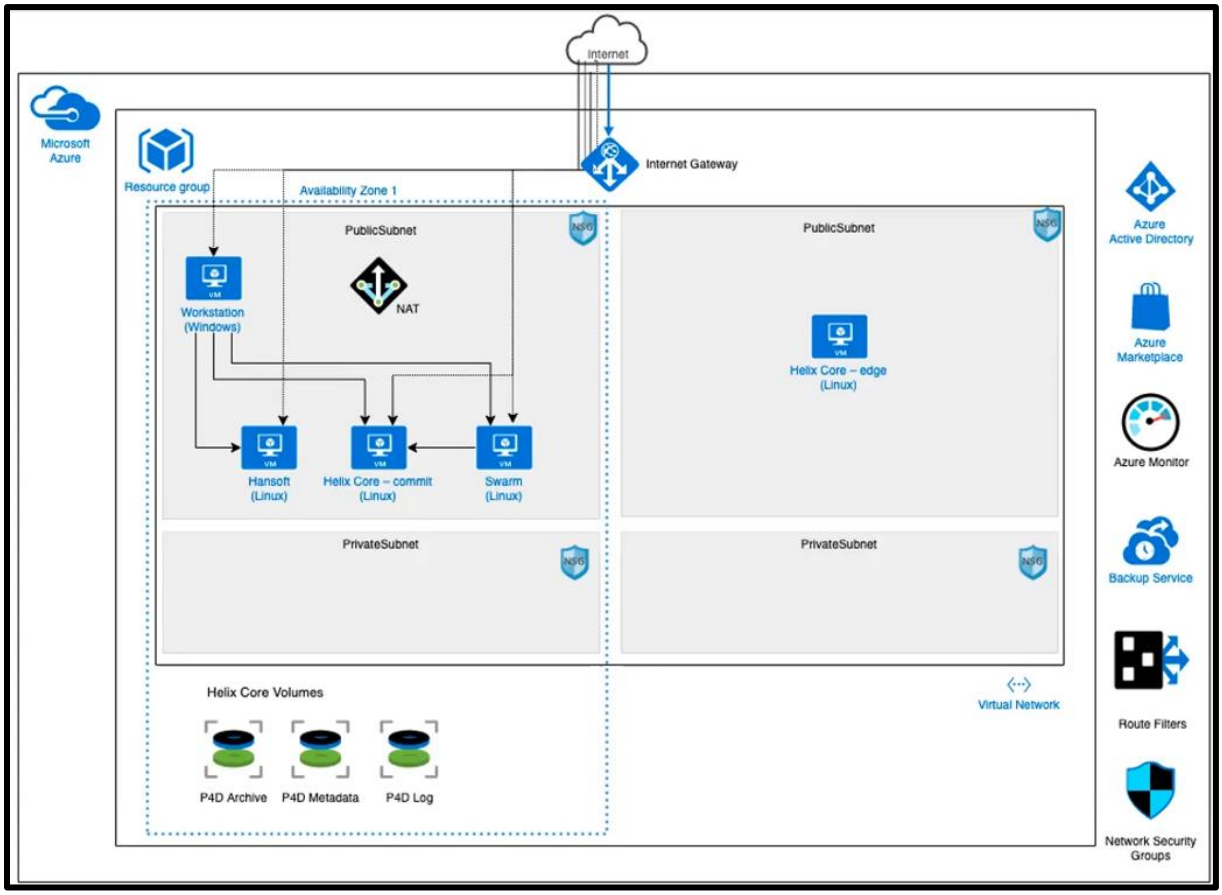

Figure 6 - Perforce ESP on Azure[4]

Following are some useful links to the Perforce ESP documentation that can help with installation and integration activities:

Perforce ESP on Azure Marketplace can be found here
Helix Core quick start guide can be found here
Helix Core integration with game engine instructions can be found here
Helix Core server admin guide can be found here
Best Practices for deploying Perforce Helix Core on Azure can be found here

[4] https://www.perforce.com/webinars/vcs/how-deploy-develop-helix-core-azure

3.5 Azure Remote Rendering

Azure Remote Rendering (ARR) is a Mixed Reality Azure service that enables users to render high-quality, interactive 3D content in the cloud and stream it in real time to devices such as the HoloLens 2. Azure offers an intuitive Software Development Kit (SDK) backed by a powerful cloud service which makes integration with existing application easy. Untethered devices (e.g., HoloLens 2) have limited computational power for rendering complex models. ARR solves this problem by moving the rendering workload to high-end GPUs in the cloud. A cloud-hosted graphics engine renders the image, encodes it as a video stream, and streams that to the target device. ARR supports hybrid rendering which allows you to render elements on any device using your preferred method UI framework e.g., Mixed Reality Toolkit (MRTK-Unity). Figure 7 below gives a high-level overview of the ARR architecture.

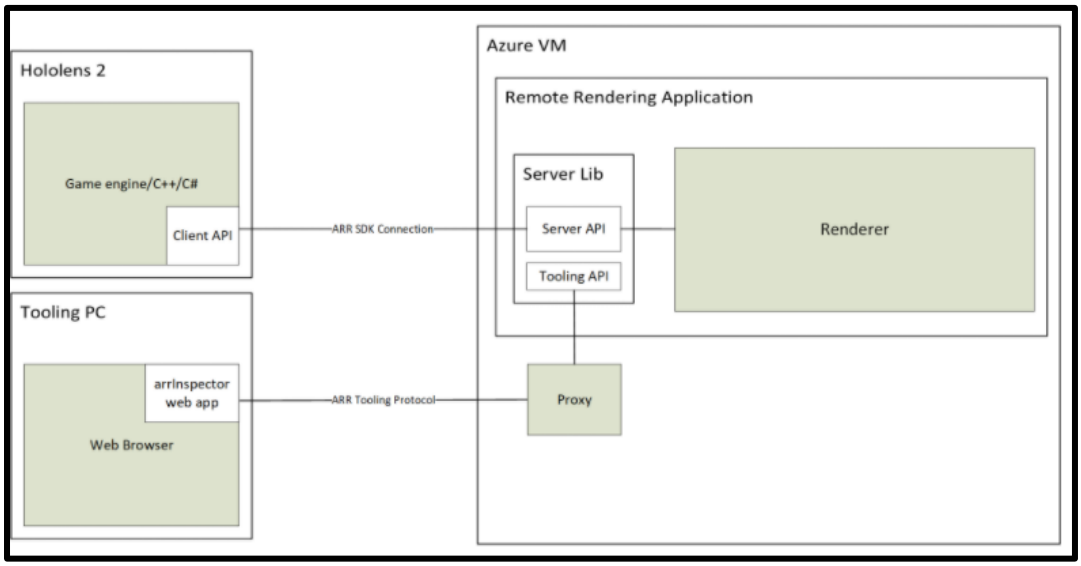

Figure 7 - ARR High-Level Architecture[5]

A full cycle for image generation involves following steps[5]:

1. Client-side: Frame setup
    a. Your code: User input is processed; scene graph gets updated
    b. ARR code: Scene graph updates and predicted head pose get sent to the server
2. Server-side: Remote rendering
    a. Rendering engine distributes rendering across available GPUs
    b. Output from multiple GPUs gets composed into single image
    c. Image is encoded as video stream, sent back to client
3. Client-side: Finalization
    a. Your code: Optional local content (UI, markers etc.) is rendered
    b. ARR code: On 'present', locally rendered content gets automatically merged with video stream

A quick start guide to render a model using Unity can be found here and a how-to guide for using the ARR service can be found here

[5] https://docs.microsoft.com/en-gb/azure/remote-rendering/overview/about

4. Remote Production Environment Deployment Using Azure

For bespoke post-production deployments, Azure features including Azure compute, virtual networking, blob storage, Azure virtual Desktops plus Azure Media services such as transcoding can be leveraged. For SaaS based options, solutions such as Avid Edit on Demand and Azure blob storage can be used.

4.1 Azure Services for Remote Production Environments

The table below details the typical Azure services required for a bespoke post-production environment:

Azure Services	Implementation Guidance
Azure Virtual Machines	Azure VM - Quick Start Azure VM - How-to Guide
Azure Blob Storage	Azure Blog Storage - Quick Start Azure Blob Storage - How-to Guide
Azure IoT Hub	Azure IoT Hub - Quick Start Azure IoT Hub - How-to Guide
Azure IoT Edge	Azure IoT Edge - Quick Start Azure IoT Edge - How-to Guide
Azure Express Route	Azure Express Route - Quick Start Azure Express Route - How-to Guide
Azure VPN Gateway	Azure VPN Gateway - Quick Start Azure VPN Gateway - How-to Guide
Azure Virtual Network	Azure Virtual Network - Quick Start Azure Virtual Network - How-to Guide
Azure Virtual Desktop	Azure Virtual Desktop – Quick Start Azure Virtual Desktop – How-to Guide
Azure Key Vault	Azure Key Vault – Quick Start Guide Azure Key Vault – How-to Guide
Azure Active Directory	Azure Active Directory – Quick Start Guide Azure Active Directory – How-to Guide
Azure API Management	Azure API Management - Quick Start Guide Azure API Management – How-to Guide

Azure Services	Implementation Guidance
Azure Media Services	Azure Media Services (encode) – Quick Start Guide Azure Media Services (encode) – How-To Guide
Azure Kubernetes Services	Azure Kubernetes Services – Quick Start Guide Azure Kubernetes Services – How-To Guide
Azure Container Registry	Azure Container Registry - Quick Start Azure Container Registry - How-to Guide
Azure Functions	Azure Functions – Quick Start Guide Azure Functions – How-To Guide
Azure Blueprints	Azure Blueprints - Quick Start Azure Blueprints - How-to Guide

Table 1 – Azure Services Implementation Guidance

4.1.1 Azure Virtual Machines

Azure VMs are one of the many types of on-demand scalable computing resources that is offered on Azure Platform. It is an IaaS service. VMs are typically used for development and test, to run applications in the cloud. Using service like Virtual Scale-Sets you can either scale up or down based on your requirements. Before deploying VMs it is always best to consider your use case, high availability, and fault tolerance, build standards, dependencies, and overall security of the virtual machines. VM size and storage would depend on your requirement.

4.1.1.1 Recommended Security Baseline Best Practices for VMs

- Deploy anti-malware for your virtual machines. You can leverage various third-party software or choose Microsoft Antimalware for Azure Cloud Services and Virtual Machines (additional details can be found here)
- Use Azure Key Vault to store your encryption keys and secrets
- Use Azure Disk Encryption functionality for your VMs (additional details can be found here)
- Use Azure Backup service for creating backups of your VMs (additional details can be found here)
- Use Azure Site Recovery that can help orchestrate replication, failover and recovery of workloads and applications (additional details can be found here)
- Consider security recommendations applicable to Virtual Networks (VNets)
- Monitor your machine state using Azure Security Centre (ASC)
- Review ASC recommendations for your VMs
- When you build custom VM images, apply the latest updates
- Centralize VM authentication using Azure AD

- Restrict access to management ports
- Use NSGs to limit network access
- Use Azure Bastion for secure management access to your VMs (additional details can be found here)

Additional security baselines and recommendations can be found here and deployment best practices can be found here

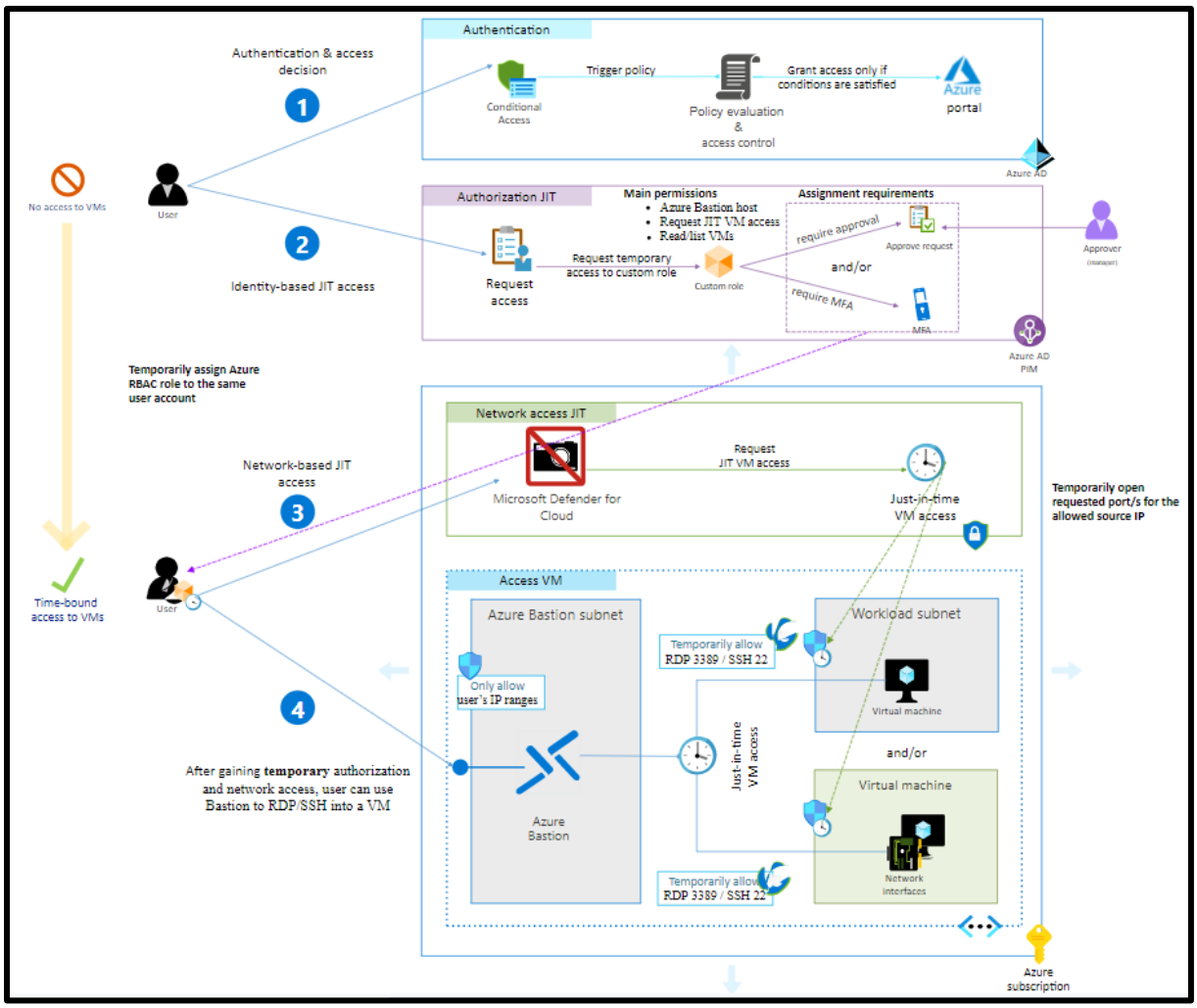

Figure 8 - Multi-Layered Protection for Azure VM[6]

Using Defense-in-depth approach, a multi-layered protection is suggested for access to Azure VMs. With this approach the user trying to access a VM in Azure is challenged with multiple layers of security controls before the user is granted access. Below are the key steps outlined in Figure 8 above:

1. **Authentication and access decisions:** User is authenticated against Azure AD for access to the Azure portal, Azure REST APIs, Azure PowerShell or Azure CLI. If authentication is successful, an Azure AD conditional access policy takes effect to verify if the user meets criteria

[6] https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/multilayered-protection-azure-vm

2. **Identity-based just-in-time (JIT) access:** Azure AD PIM assigns the user a custom role of type eligible which gives them time bound role for required resources. User can request activation of this role within the specified period which will trigger other actions in the background e.g., approval workflow, MFA etc.
3. **Network based just-in-time (JIT) access:** Once the user is authenticated and authorized, the custom role is linked to user's identity. This allows the user to then request JIT VM access which open a connection via the Azure Bastion subnet (RDP or SSH) directly to the VM NIC or VM NIC subnet
4. **Connecting to Azure VM:** Using a temporary token, the user accesses Azure Bastion, which then allows a time bound internal access to the Azure VM on either RDP or SSH

4.1.2 Azure Blob Storage

Azure Blob Storage is an object storage solution for cloud. It is optimized to store massive amounts of unstructured data (e.g., text, binary etc.). Users and applications can access objects in Blob storage via HTTP/HTTPS from anywhere. Objects in Blob storage are accessible via the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. Some of the common use cases for Blob storage includes:

- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Writing to log files
- Storing data for backup and restore, disaster recovery, and archiving
- Storing data for analysis by an on-premises or Azure-hosted service

Blob Storage offers three types of resources:

- Storage account – provides unique namespace in Azure for your data
- Container – organizes a set of blobs (like a directory in a file system)
- Blob

Figure 9 – Blob Storage Resources illustrates the relationship between these resources.

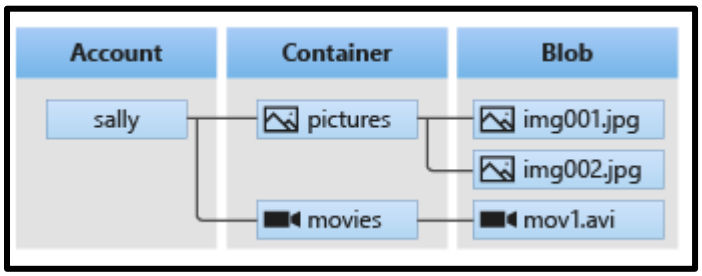

Figure 9 - Blob Storage Resources[7]

[7] https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

4.1.2.1 Recommended Security Baseline Best Practices for Blob Storage

- Use Azure Resource Manager deployment model to create a new storage account
- Enable Azure Defender for all your storage accounts (additional details can be found here)
- Turn on soft delete for blobs to enable data recovery (additional details can be found here)
- Turn on soft delete for containers to enable data recovery (additional details can be found here)
- Lock storage account using Azure Resource Manager lock to prevent accidental or malicious deletion or configuration changes (additional details can be found here)
- Configure legal holds and time-based retention policies to store blob data in a WORM (Write Once, Read Many) state for business critical data (additional details can be found here)
- Enforce use of HTTPS access only for your storage account
- Grant limited access to your storage account using Shared Access Signatures (SAS) (additional details can be found here)
- Use Azure AD to authorize access to blob data
- Use Azure Key Vault to store your account access keys
- Rotate account keys periodically
- Consider principal of least privilege when assigning permissions to a SAS
- Disable anonymous public read access to containers and blobs
- Configure firewall rules to limit access to your storage account and allow trusted Microsoft services on the firewalls
- Use Private Endpoints for connectivity between VNet and storage account (additional details can be found here)
- Enable Azure Storage logging to track how each request made against Azure Storage was authorized (additional details can be found here)
- Setup alerts in Azure Monitor

Additional security baselines and recommendations can be found here and performance and scalability checklist can be found here.

4.1.3 Azure IoT Hub

The Internet of Things (IoT) is typically defined as a network of physical devices that connect to and exchange data with other devices and services over the Internet or other communication network. Azure IoT Hub is a managed service hosted in the cloud that acts as a central message hub for communication between an IoT application and its attached devices. Almost any device can be connected to an IoT Hub. It can support several messaging patterns including device-to-cloud telemetry, uploading files from devices, and request-reply methods to control your devices from the cloud. Some of the common integrations of IoT Hub with Azure services include:

- Azure Event Grid to enable your business to react quickly to critical events in a reliable, scalable, and secure manner
- Azure Logic Apps to automate business processes
- Azure Machine Learning to add machine learning and AI models to your solution
- Azure Stream Analytics to run real-time analytic computations on the data streaming from your devices

4.1.3.1 Recommended Security Baseline Best Practices for Azure IoT Hub

- To secure IoT Hub to a private networking environment use Azure Private Link (additional details can be found here)
- Depending on the protocol used (MQTT, AMQP, HTTPS, WebSocket), IoT Hub requires specific service ports to be open (additional details can be found here)
- Protect your IoT Hub resources against attacks from external network attacks e.g., DDoS, application-specific, malicious internet traffic etc. using Azure Firewall and Azure DDoS (additional details can be found here and here)
- Use Azure Virtual Network Service Tags to define network access controls on NSGs and Azure Firewalls protecting IoT Hub (additional details can be found here)
- Standardize Azure Active Directory as the central identity and authentication system (additional details can be found here)
- Use managed identities with IoT Hub instead of creating service principals to access other resources (additional details can be found here)
- Use Azure AD single sign-on (SSO) for application access (additional details can be found here)
- Protect and limit highly privileged users (additional details can be found here)
- Enable threat detection for Azure resources (additional details can be found here)
- Enable logging for Azure network activities (additional details can be found here)

Additional security baseline details can be found here and security best practices for IoT can be found here

4.1.4 Azure IoT Edge

Azure IoT Edge moves cloud analytics and custom business logic to devices so that your organization can focus on business insights instead of data management. Azure IoT Edge is made up of three components:

- IoT Edge modules – these are containers that run Azure services, third-party services, or your own code. Modules are deployed to IoT Edge devices and execute locally on those devices
- IoT Edge runtime – it runs on each IoT Edge device and manages the modules deployed to each device
- IoT Edge Cloud Interface - it enables you to remotely monitor and manage IoT Edge devices

4.1.4.1 Recommended Security Baseline Best Practices for Azure IoT Edge

At the time of writing this document, there is no specific Azure recommended security baseline, but Azure provides with recommended security guidance for securing Azure IoT Edge here

4.1.5 Azure Virtual Network (VNet)

Azure Virtual Network (VNet) is the key component for deploying private network in Azure. It enables secure communication between VMs as well to internet and on-premises networks. It offers benefits like scalability, availability, and isolation. Additionally, it supports network traffic

filtering, routing, segmentation, and integration with other Azure services. Key VNet concepts include:

- Address space – a custom private IP address space must be defined (using RFC 1918 addresses)
- Subnets – it enables you to segment your network and allocate a portion of address space to each subnet/segment. Resources within subnets can be secured using NSGs
- Regions – VNet is scoped to a single region/location but virtual networks from different regions can be connected using Virtual Network peering
- Subscription – VNet is scoped to a subscription, multiple VNet can be deployed within each subscription and region

4.1.5.1 Recommended Security best practices for VNet security

- Centralize management of core network functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing
- Centralize governance of network security elements e.g., ExpressRoute, subnet provisioning, IP addressing etc.
- Do not assign allow rules with broad ranges and use smaller subnets instead
- Use NSGs to protect against unsolicited traffic into Azure subnets
- Simplify network security group rule management by defining Application Security Groups (additional details can be found here)
- Give conditional access to resources based on device, identity, assurance, network location etc. (additional details can be found here)
- Lockdown inbound traffic to Azure using just-in-time VM access (additional details can be found here)
- Consider Azure native controls like Azure Firewall and WAF with Application gateway to protect your perimeter network
- Use Site-to-Site VPN or ExpressRoute to avoid exposure to internet
- Disable direct RDP/SSH access to virtual machines from internet and either dedicated connection from on-premises or bastion-hosts with restricted number of users
- Use Azure Private Link to access Azure PaaS services (e.g., Azure Storage, SQL Database etc.)

Additional security baselines and recommendations for Virtual Networks can be found here and deployment best practices can be found here.

4.1.6 Azure ExpressRoute

Azure ExpressRoute is used to extend your on-premises network into Microsoft Cloud services like Azure and Office365 over a private dedicated connection. It can be an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections do not go over internet and hence provides higher level of security. Different types of ExpressRoute Connectivity models can be found here.

Figure 10 – Azure ExpressRoute Connectivity illustrates connectivity from on-premises network to Azure cloud using Azure ExpressRoute. The Microsoft edge element in the diagram is the entry point for ExpressRoute circuits into Microsoft's network.

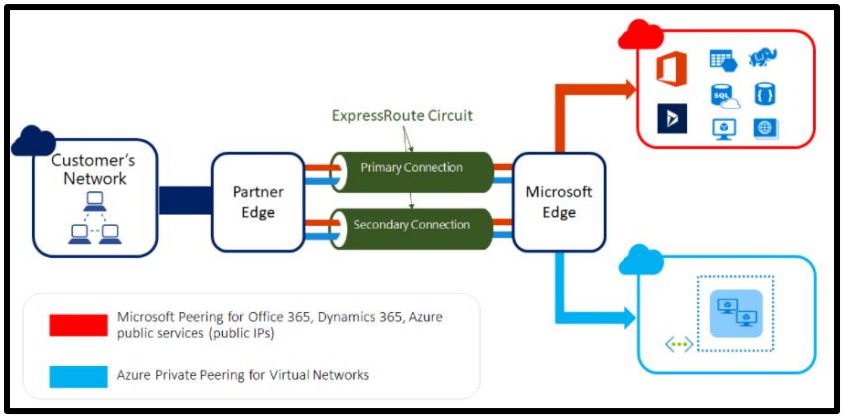

Figure 10 - Azure ExpressRoute Connectivity[8]

4.1.6.1 Recommended Security Baseline Best Practices for ExpressRoute

- Deploy standard security configurations for ExpressRoute using Azure Policy (additional details can be found here)
- Use tags for your Azure ExpressRoute instances to provide metadata and logical organization
- Use Azure Activity Log to monitor network resource configurations and detect changes to network resources related to ExpressRoute connections. Use Azure Monitor to trigger alerts ((additional details for activity log can be found here and for Azure Monitor here)
- Enable Azure Activity Log diagnostic settings and send the logs to a Log Analytics workspace, Azure event hub, or Azure storage account for archive (additional details for enabling diagnostic settings is here)
- Set log retention period for Log Analytics in Azure Monitor based on your organization's retention policy
- Enable alerts for anomalous activities using Azure Monitor
- Maintain an inventory of the user accounts that have administrative access to the control plane (e.g., Azure portal) of your Azure ExpressRoute resources.
- Change default passwords where applicable
- Use dedicated admin accounts
- Log and alert on suspicious activities from administrative accounts
- Use Conditional Access Named Locations to allow access to the Azure portal from only specific logical groupings of IP address ranges or countries/regions (additional details can be found here)
- Use Azure AD as the central authentication and authorization system

Additional security baseline recommendations can be found here and ExpressRoute deployment best practices can be found here.

[8] https://docs.microsoft.com/en-ca/azure/expressroute/expressroute-introduction

4.1.7 Azure VPN Gateway

VPN gateway is a virtual network gateway that can be used to send encrypted traffic between an Azure virtual network and an on-premises location using public internet. It can also be used to send encrypted traffic between Azure VNets using Microsoft's network. A virtual network gateway is made of two or more VMs that are deployed within a gateway subnet. These VMs are automatically created when you create a virtual network gateway, and they contain routing tables and run specific gateway services.

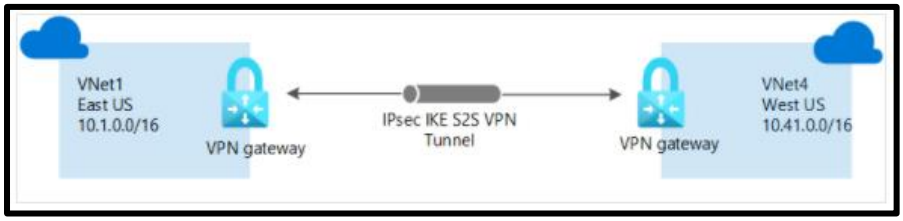

Figure 11 – VNet-to-VNet VPN[9]

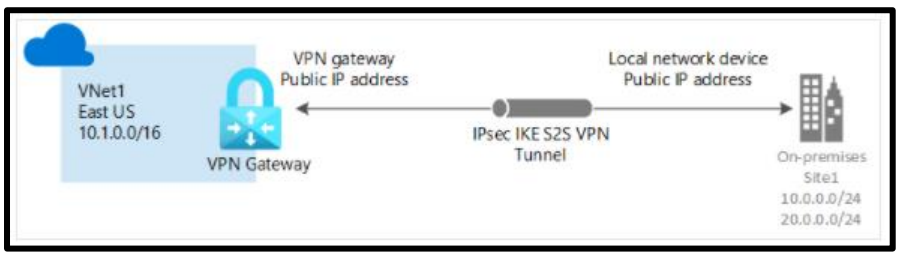

Figure 12 – Site-to-Site VPN[9]

4.1.7.1 Recommended Security Baseline Best Practices for VPN Gateway

- Implement security for internal traffic using NSGs, Azure Firewall and network segmentation
- Protect your VPN Gateway resources against attacks from external networks e.g., DDoS, malicious internet traffic (additional details can be found here)
- Azure VPN uses Azure AD as its default identity and hence ensure Azure AD is standardized and governed for IAM
- Forward VPN gateway logs to your SIEM platform for monitoring and threat detection
- Enable the NSG flow log capability in your deployed VPN gateway (additional details can be found here)
- Configure custom cryptographic policies for VPN gateway using Azure portal, PowerShell or Azure CLI (additional details cryptographic requirements can be found here)

Additional details for Security baseline applicable to VPN Gateway can be found here.

[9] https://docs.microsoft.com/en-us/azure/vpn-gateway/design

4.1.8 Azure Kubernetes Service

Azure Kubernetes Service (AKS) is a managed Kubernetes offering which provides simplified container-based application deployment and management.

Kubernetes is a rapidly evolving platform that manages container-based applications and their associated networking and storage components. Kubernetes focuses on the application workloads, not the underlying infrastructure components. Kubernetes provides a declarative approach to deployments, backed by a robust set of APIs for management operations.

AKS provides a managed Kubernetes service that reduces the complexity of deployment and core management tasks, like upgrade coordination. The Azure platform manages the AKS control plane, and you only pay for the AKS nodes that run your applications. AKS is built on top of the open source Azure Kubernetes Service Engine. Some of the common use cases for AKS include:

- Running of containerized media specific applications. For example, Avid Media Central runs Kubernetes Managed Docker Container Structure.
- Running of in-house developed media specific applications.

To run applications and supporting services, you need a Kubernetes *node*. An AKS cluster has at least one node, an Azure virtual machine (VM) that runs the Kubernetes node components and container runtime. An AKS cluster is made up of the following resources:

- Kubelet – The Kubernetes agent that processes the orchestration requests from the control plane and scheduling of running the requested containers

- Kube-proxy – Handles virtual networking on each node. The proxy routes network traffic and manages IP addressing for services and pods

- Container Runtime - Allows containerized applications to run and interact with additional resources, such as the virtual network and storage. AKS clusters using Kubernetes version 1.19+ for Linux node pools use containerd as their container runtime. Beginning in Kubernetes version 1.20 for Windows node pools, containerd can be used in preview for the container runtime, but Docker is still the default container runtime. AKS clusters using prior versions of Kubernetes for node pools use Docker as their container runtime

Figure 13 – AKS cluster illustrates the relationship between these resources

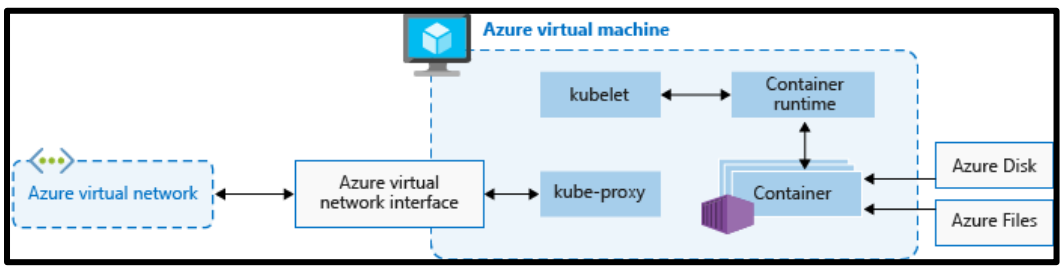

Figure 13 - Azure Kubernetes Service[10]

[10] https://docs.microsoft.com/en-gb/azure/aks/concepts-clusters-workloads

4.1.8.1 Recommended Security Baseline Best Practices for AKS Clusters

- Protect Azure resources within virtual networks (additional details can be found here)
- Use Microsoft Defender for Cloud and follow its network protection recommendations to secure the network resources being used by your Azure Kubernetes Service (AKS) clusters (additional details can be found here)
- Use an Azure Application Gateway enabled Web Application Firewall (WAF) in front of an AKS cluster to provide an additional layer of security by filtering the incoming traffic to your web applications (additional details can be found here)
- Deny communications with known malicious IP addresses (additional details can be found here)
- Deploy network-based intrusion detection/intrusion prevention systems (IDS/IPS)
- Use automated tools to monitor network resource configurations and detect changes (additional details can be found here)
- Enable audit logging for Azure resources (additional details can be found here)
- Onboard your Azure Kubernetes Service (AKS) instances to Azure Monitor and configure diagnostic settings for your cluster (additional details can be found here)
- Use Azure Kubernetes Service (AKS) together with Microsoft Defender for Cloud to gain deeper visibility into AKS nodes
- Install and enable Microsoft Anti-malware for Azure to AKS virtual machines and virtual machine scale set nodes. Review alerts in Microsoft Defender for Cloud for remediation

Additional details for Security baseline applicable to AKS can be found here

4.1.9 Azure Functions

Azure Functions is a cloud service available on-demand that provides all the continually updated infrastructure and resources needed to run applications. Azure Functions enables customers to focus on the pieces of code that matter most, and Azure Functions handles the rest. Functions provides serverless compute for Azure.

Some of the common use cases for Azure Functions include:

- Web API’s
- Respond to database changes
- Manage message queues

4.1.9.1 Recommended Security Baseline Best Practices for Azure Functions

- Implement security for internal traffic (additional details can be found here)
- Use Azure Private Link to enable private access to Azure Functions from your virtual networks without crossing the internet (additional details can be found here)
- Protect your Azure Functions resources against attacks from external networks, including distributed denial of service (DDoS) attacks, application-specific attacks, and unsolicited and potentially malicious internet traffic (additional details can be found here)
- Follow the best practices for DNS security to mitigate against common attacks like dangling DNS, DNS amplifications attacks, DNS poisoning and spoofing, etc.
- Standardize Azure Active Directory as the central identity and authentication system
- Manage application identities securely and automatically (additional details can be found here)

- Use Azure AD single sign-on (SSO) for application access
- Monitor and alert on account anomalies

Additional details for Security baseline applicable to AKS can be found here

4.1.10 Azure Container Registry

Azure Container Registry is a managed, private Docker registry service based on the open-source Docker Registry 2.0. It is used to create and maintain Azure container registries to store and manage private Docker container images and related artifacts.

Azure container registries can be used with your existing container development and deployment pipelines or use Azure Container Registry Tasks to build container images in Azure. It supports build on demand, or fully automate builds with triggers such as source code commits and base image updates.

4.1.10.1 Recommended Security Baseline Best Practices for Azure Functions

- Implement security for internal traffic (additional details can be found here)
- Container registries should not allow unrestricted network access (additional details can be found here)
- Use Azure Private Link to enable private access to Container Registry from your virtual networks without crossing the internet (additional details can be found here)
- Protect your Azure Container Registry resources against attacks from external networks (additional details can be found here)
- Standardize Azure Active Directory as the central identity and authentication system (additional details can be found here)
- Protect and limit highly privileged users (additional details can be found here)
- Monitor for unauthorized transfer of sensitive data (additional details can be found here)
- Encrypt sensitive data at rest (additional details can be found here)
- Use the Microsoft Defender for Cloud built-in threat detection capability and enable Microsoft Defender for your Container Registry resources (additional details can be found here)

4.2 Azure Security Services for Remote Production Environments

Security is an important consideration when deploying services in cloud and Microsoft Azure platform gives security priority by offering critical native services which can be leveraged to ensure your services are deployed securely on Azure. Table 2 – Azure Security Services Implementation Guidance below lists some of the important Azure native security services applicable for post-production workflow.

Azure Security Services	Implementation Guidance
Network Security Groups (NSGs)	NSG - Quick Start NSG - How-to Guide
Azure AD	Azure AD - Quick Start Azure AD - How-to Guide
Microsoft Defender for Cloud (Formerly known as Azure Security Center)	Microsoft Defender for Cloud – Quick Start Microsoft Defender for Cloud – How-to Guide
Microsoft Sentinel (Formerly known as Azure Sentinel)	Azure Sentinel - Quick Start Azure Sentinel - How-to Guide
Azure Policy	Azure Policy - Quick Start Azure Policy - How-to Guide
Azure Key vault	Azure Key Vault - Quick Start Azure Key Vault - How-to Guide
Microsoft Defender for Cloud (Formerly known as Azure Defender)	Azure Defender – Quick Start Guide Azure Defender – How-to Guide
Azure DDoS Protection Standard	Azure DDoS - Quick Start Azure DDoS - How-to Guide
Azure Firewall	Azure Firewall - Quick Start Azure Firewall - How-to Guide
Network Watcher	Network Watcher - Quick Start Network Watcher - How-to Guide
Bastion Hosts	Bastion Hosts - Quick Start Bastion Hosts - How-to Guide
Azure Monitor	Azure Monitor - Quick Start Azure Monitor - How-to Guide

Table 2 – Azure Security Services Implementation Guidance

4.2.1 Azure Network Security Groups (NSG)

Azure NSGs are used to filter network traffic to and from Azure resources in an Azure VNet. It contains deny or allow rules for inbound and outbound traffic. For each rule you define source, destination, port, and protocol. Rules are processed in priority order between 100 and

4096, lower numbers are processed before higher numbers. Once traffic matches a rule, processing stops. NSGs are stateful in nature - a flow record is created for every connection, state of the flow record either allows or denies communication.

Following default rules are created when you create a Network Security Group:

- AllowVNetInBound – VNet to VNet any/any allow rule
  [Allows all inbound traffic from any source VM to Destination VM within the VNet]
- AllowAzureLoadBalancerInBound – AzureLoadBalancer to ANY, any/any allow rule
  [Allows LoadBalancer traffic to Destination VM within the VNet]
- DenyAllInbound – Any to Any, any/any deny rule
  [Deny any source traffic from outside the VNet]
- AllowVnetOutBound – VNet to VNet any/any allow rule
  [Allows all outbound traffic from any source VM to Destination VM within the VNet]
- AllowInternetOutBound – Any to Internet, any/any allow rule
  [Allows all traffic outbound from VM to Internet]
- DenyAllOutBound – Any to Any, any/any deny rule
  [Deny traffic from VM outbound to any destination outside of the VNet]

It should be noted that you cannot remove the default rules, but you can override them by creating rules with lower priorities.

For other Azure platform considerations for NSGs, you can find more information here and to manage your NSGs details are here

4.2.1.1 Recommended Security Baseline Best Practices for NSGs

- Understand the rule priorities and how it affects your traffic flow
- Use a proper naming convention to identify rules and their remit
- Use service tags to minimize complexity (additional details can be found here)
- Use Application Security Groups to group VMs and define security policies based on those groups (additional details can be found here)
- Enable NSG flow logs (additional details can be found here)

4.2.2 Azure Active Directory (AD)

Azure AD is Microsoft's cloud-based identity and access management (IAM) service which helps users and services to authenticate and authorize before accessing resources. It is widely used to automatically help protect user identities and credentials, and to meet an organization's access governance requirements. It is commonly used by IT admins to manage user and service access, Application developers to add single sign-on (SSO) capabilities in application and SaaS services like Microsoft 365, Azure, Dynamics CRM etc. There are additional paid capabilities that can be considered by upgrading to either Azure AD Premium P1 or Premium P2 licenses, additional details can be found here.

Some of the key features (depending on the type of license you select) include:

- Application Management
- Authentication
- Azure AD for developers
- Business-to-Business (B2B – external or guest users)
- Business-to-Customer (B2C – how users sign-in when using your services)
- Conditional Access
- Device Management
- Domain Services
- Enterprise Users
- Hybrid identity
- Identity governance
- Identity Protection
- Managed identities for Azure resources
- Privileged identity management (PIM)
- Reports and Monitoring

4.2.2.1 Recommended Security Baseline Best Practices for Azure AD

- Enable MFA for your AD users (additional details can be found here)
- Enable security default settings (additional details can be found here)
- Review dependency on legacy authentication and where applicable block legacy authentication (additional details can be found here)
- Review your identity secure score and list of recommended improvements (additional details can be found here)
- Secure remote worker identities by leveraging recommended practices and checklist items here
- Implement security for internal traffic by network segmentation and implementing NSG and/or Azure Firewall rules
- Use Azure ExpressRoute or Azure VPN to create private connections between Azure datacenters and on-premises infrastructure
- Use Azure Private Link to enable private access to Azure AD from your VNets without crossing the internet (additional details can be found here)
- Use WAF, DDoS protection, Azure Content Delivery Network (CDN) to protect against application layer attacks
- Simplify network security rules (NSG or Azure Firewall)
- Conduct regular attack simulation (refer to Microsoft Cloud Penetration Testing Rules of Engagement)

Additional details for Azure AD best practices, security baseline, deployment guidance and architecture can be found here

4.2.3 Microsoft Defender for Cloud

Microsoft Defender and Azure Defender are now known as Microsoft Defender for Cloud. Defender for cloud provides unified security management and threat protections across your hybrid and multi-cloud workloads. It is a tool for security posture management and threat protection, and it can be used for hardening of your resources.

Defender for cloud is available in two modes:

- Defender for Cloud (free version): It can be enabled for free via the Defender dashboard in Azure portal. It provides with secure score, security policy, continuous security assessment and actionable security recommendations to help you protect your Azure resources
- Defender for Cloud (enhanced security features – paid version): This extends capabilities of free mode to other workloads running in private or other public cloud platforms. Other key functionalities include – Defender for endpoint for comprehensive endpoint detection and response (EDR), vulnerability scanning for virtual machines and container registries, multi-cloud security, hybrid security for on-premises coverage, threat protection alerts, track compliance, access and application controls, container security features and Azure-native breadth threat protection for all your Azure resources. Enhanced protections can be enabled as per instructions here

Figure 14 – Microsoft Defender for Cloud Overview shows the overview screen (free version) that you would see in your Azure portal. To enable Defender for Cloud on all subscriptions refer to instructions here.

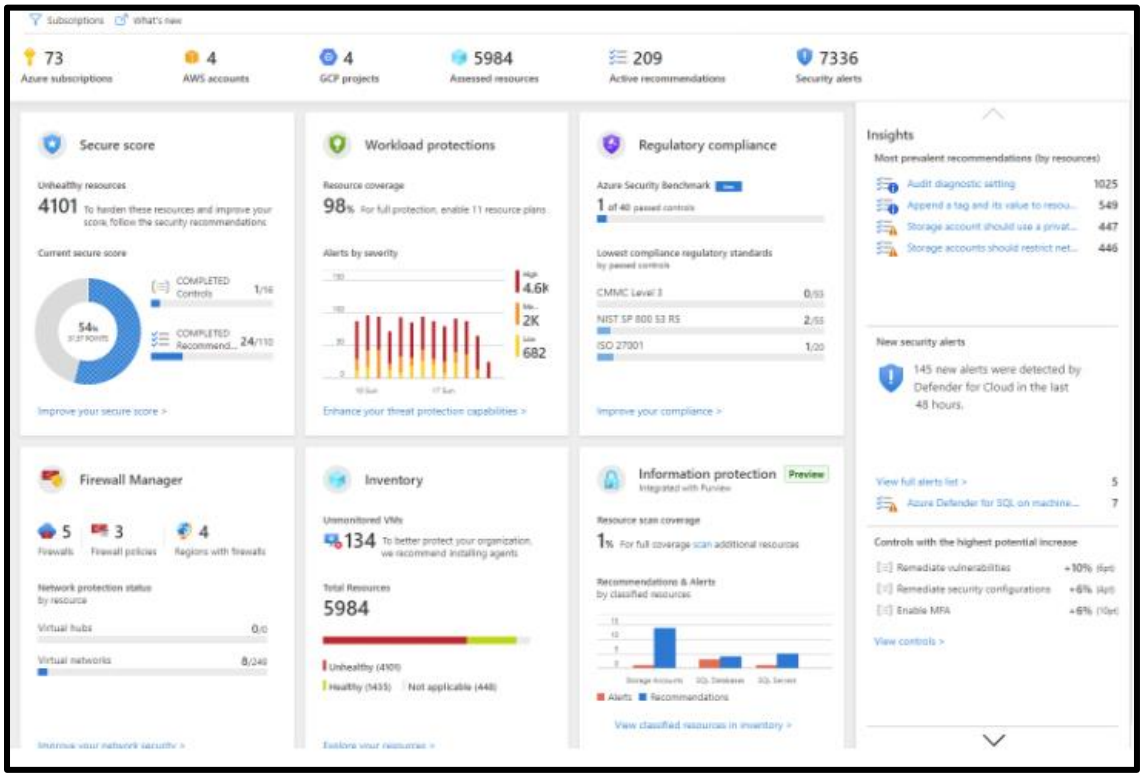

Figure 14 - Microsoft Defender for Cloud Overview[11]

4.2.3.1 Recommended Security Baseline Best Practices for Microsoft Defender for Cloud

- Monitor and review your security recommendations regularly (additional details can be found here)
- Remediate any security recommendations
- Use Defender for Cloud to prevent misconfigurations by leveraging deny/enforce options (additional details can be found here)

[11] https://docs.microsoft.com/en-us/azure/security-center/get-started

- Automate responses to security recommendations (additional details can be found here)
- Use Defender for Cloud to manage your multi-cloud environment
- Use security scores within the dashboard to continuous monitor and continuous remediate any security issues
- Use RBAC to grant access to Defender for Cloud portal and ensure that the user accounts are reviewed regularly (additional details can be found here)
- If you use a separate SIEM platform, then ensure logs from Defender for Cloud portal are forwarded to your SIEM tool to setup custom threat detection
- Set the required log retention period (based on your organization's policy) for any system used to store Microsoft Defender for Cloud logs

4.2.4 Microsoft Sentinel

Microsoft Sentinel (formerly known as Azure Sentinel) is a scalable, cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution. It provides with intelligent security analytics and threat intelligence across your environment acting as a single solution for alert detection, threat visibility, proactive hunting, and threat response. Some of the key capabilities of Microsoft Sentinel include:

- Collect Security data across your enterprise
- Detect threats with vast threat intelligence
- Investigate critical incidents guided by Artificial Intelligence (AI)
- Respond rapidly and automate protection

Figure 15 – Microsoft Sentinel Data Sources below shows some of the data sources that can ingest data from into Sentinel platform.

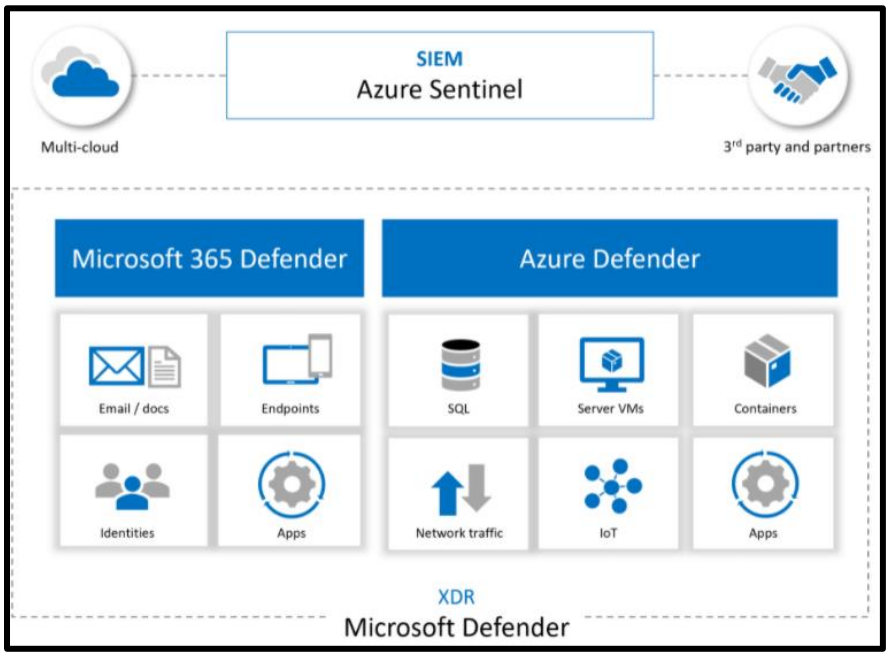

Figure 15 – Microsoft Sentinel Data Sources[12]

[12] https://docs.microsoft.com/en-us/azure/sentinel/best-practices

4.2.4.1 Recommended Security Baseline Best Practices for Azure Sentinel

- Complete pre-deployment activities and prerequisites before deploying Microsoft Sentinel (additional details can be found here)
- Setup weekly tasks for workbook updates (here), Sentinel GitHub repository review (here) and Sentinel platform auditing (here)
- Setup monthly tasks to review user access (here) and log analytics workspace review (here)
- Use Sentinel feature for incident management (additional details can be found here)
- Use separate Sentinel instances for each region if required to meet any compliance requirements

Additional details for Microsoft Sentinel security baseline can be found here

4.2.5 Azure Advisor

Azure Advisor is a personalized cloud consultant that helps you to follow best practices to optimize your Azure Deployments. By analyzing your resource configuration and usage telemetry it recommends solutions that can help you improve cost effectiveness, performance, reliability, and security of your Azure resources. It can be accessed via the Azure Portal by either locating it in the navigation menu or using the search function (See Figure 16 – Azure Advisor).

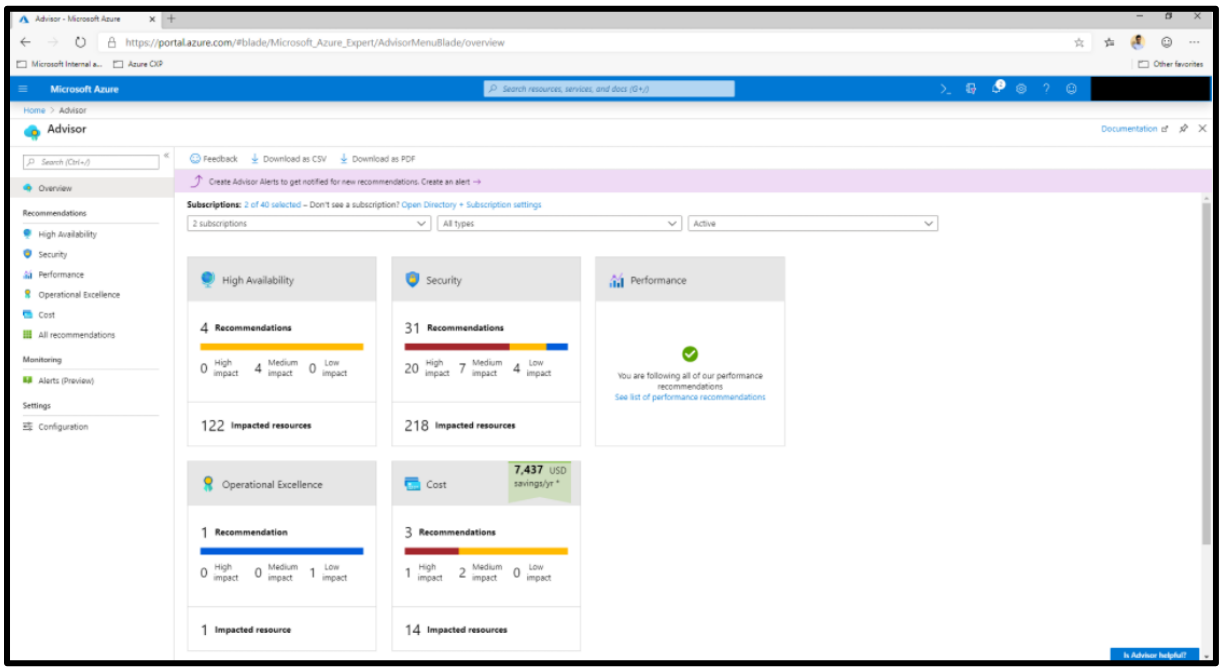

Figure 16 - Azure Advisor[13]

It gives you options to postpone or dismiss any recommendations so depending on the applicability to your environment, you can decide to take the appropriate actions.

[13] https://docs.microsoft.com/en-us/azure/advisor/advisor-overview

4.2.5.1 Recommended Security Baseline Best Practices for Azure Advisor

- Standardize Azure AD as the central identity and authentication system (additional details can be found here)
- User Azure AD single sign-on for application access (additional details can be found here)
- Azure Advisor uses Azure Active Directory (Azure AD) accounts to manage its resources, review user accounts and access assignment regularly to ensure the accounts and their access are valid (additional details can be found here)
- Use privileged access workstations e.g., Azure Bastion
- Azure Advisor is integrated with Azure role-based access control (Azure RBAC) to manage its resources. Use Azure RBAC to manage Azure resource access through role assignments (additional details can be found here)

Additional security baseline recommendations can be found here

4.2.6 Azure Key Vault

Azure Key Vault can be used for secrets management (securely store and tight control access to tokens, passwords, certificates, API keys etc.), key management (create and secure encryption keys) and certificate management (provision, manage and deploy public and private TLS/SSL certificates). It has two tiers – standard which encrypts with software key and premium tier which includes hardware security module (HSM) protected keys.

Following are some advantages using Azure Key Vault:

- Centralize application secrets
- Securely store secrets and keys
- Monitor access and use
- Simplified administration of application secrets
- Integrates with other Azure services

Figure 17 – Key Vault Request Operation Flow below illustrates the complete authentication and request flow to the Key Vault from an application calling “Get Secret” API.

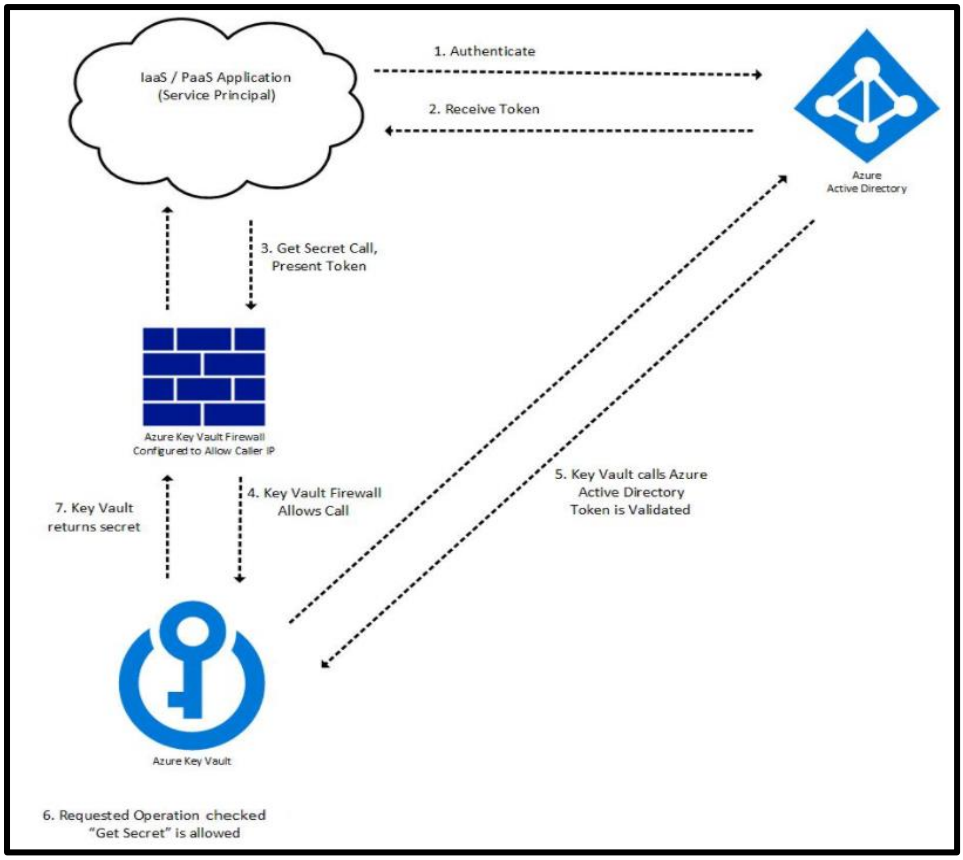

Figure 17 – Key Vault Request Operation Flow[14]

4.2.6.1 Recommended Security Baseline Best Practices for Azure Key vault

- Restrict access to vault by specifying source IP addresses when using VNet service endpoints (additional details can be found here)
- Where possible make use of Azure Private Link to access Key Vault from your VNet (additional details can be found here)
- Use Azure AD conditional access policy to restrict user access (additional details can be found here)
- Azure Key Vault Firewall is disabled by default, this should be enabled and configured with only required access flows (additional details can be found here)
- Disable Azure Key Vault public network access
- Enable resource logs in Key Vault – Azure Monitor can be used to enable resource logging and data collection (additional details can be found here)
- Key Vault keys and secrets should have expiration dates
- Key Vaults should have soft delete and purge protection enabled (additional details can be found here)

Additional details for security baseline applicable to Azure Key Vault can be found here

[14] https://docs.microsoft.com/en-us/azure/key-vault/general/authentication

4.2.7 Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. It is used to create, assign, and manage policies which help to ensure that your resources are compliant with your organization's standards and policy. Properties of resources in Azure are compared to business requirements (rules) using Azure Policy which are described in JSON format known as policy definitions. Rules can be grouped together and are often referred to as policy initiative (or a policySet). Policy definition or initiative is assigned to any scope of resources in Azure including management groups, subscriptions, resource groups or individual resources. Azure Policy data and objects are encrypted at rest.

4.2.7.1 Recommended Security Baseline Best Practices for Azure Policy

- Azure Policy uses Azure AD for IAM and hence you should standardize AD as the central identity and authentication system
- Azure Policy uses Azure-managed identities for services and automation accounts, hence Azure-managed identity feature should be used
- Use MFA and Passwordless for Azure AD based access
- Azure Policy definitions could contain credentials and secrets; hence it is recommended to audit for credentials (additional details can be found here)
- Forward logs from Azure Policy to your SIEM platform for monitoring and threat detection

Complete list of security baseline guidance for Azure Policy can be found here

4.2.8 Azure Firewall

Azure Firewall is a full stateful network security service that can be used to protect virtual network resources in your Azure environment. It has built-in HA and unrestricted cloud scalability. It is fully integrated with Azure Monitor for logging and analytics. It enables you to centrally create, enforce and log network and application connectivity policies across subscriptions and virtual networks. Following are key features:

- Built-in HA
- Availability Zones
- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN and Service tags
- Threat intelligence
- Outbound SNAT and inbound DNAT support
- Forced tunnelling
- Web Categories

Additionally, Azure Firewall Premium is also available with next generation firewall capabilities e.g., TLS inspection, IDPS, URL filtering etc.

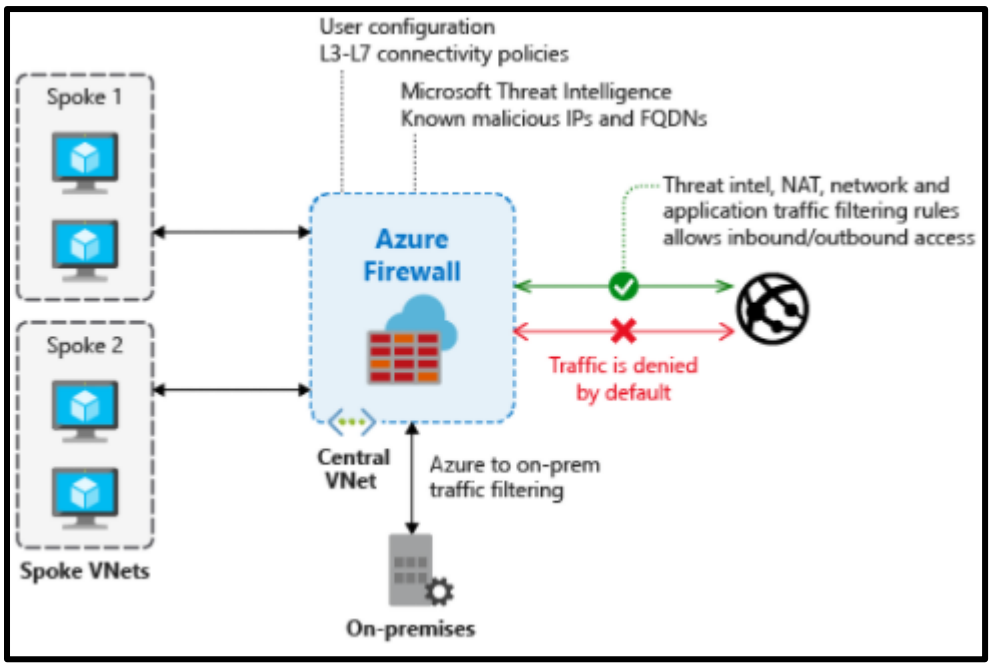

Figure 18 – Azure Firewall[15]

4.2.8.1 Recommended Security Baseline Best Practices for Azure Firewall

- Use Microsoft Defender for Cloud and follow recommendations provided for network resources related to Azure Firewall
- Network Watcher should be enabled to monitor and diagnose conditions at network scenario level
- Enable Threat-Intelligence filtering to alert and deny traffic from/to known malicious IP addresses and domains (additional details can be found here)
- Use Azure Firewall service tags to simplify rules (additional details can be found here)
- Azure Firewall Manager can be used to achieve standardization of security configurations (additional details can be found here)
- Use Azure Activity Log to monitor resource configurations and detect changes to your Azure Firewall resources (additional details can be found here)
- Configure central security log management by forwarding your Azure resources log data to your SIEM platform
- Use Microsoft Defender for Cloud for monitoring and alerting on anomalous activity found in security logs and events
- Use PAWs (privileged access workstations) with MFA to log into and configure Azure Firewall and related resources (additional details can be found here)

Additional details for Azure Firewall security baseline can be found here

[15] https://docs.microsoft.com/en-us/azure/firewall/threat-intel

4.2.9 Azure DDoS Protection

Distributed Denial of Service (DDoS) attacks attempt to exhaust an application or system's resources, making them unavailable for legitimate users. Any application or endpoint system that is publicly reachable over internet is susceptible to DDoS attacks. Azure DDoS Protection (Basic) is the basic protection for your Azure environment with no additional cost. It requires no user configuration or application changes. It is automatically tuned to help protect your specific Azure resources in a virtual network. It does not store any customer data. Azure DDoS protection (Standard) provides enhanced capabilities at additional cost. Following are some key features for Standard protection:

- Native platform integration
- Turnkey protection
- Always-on traffic monitoring
- Adaptive tuning
- Multi-layered protection
- Extensive mitigation scale
- Attack analytics
- Attack metrics
- Attack Alerting
- DDoS Rapid Response
- Cost guarantee

Figure 19 – Azure DDoS Protection (Basic vs Standard) below shows a comparison between the two offerings.

Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee		●
Cost Protection		●
Mitigation policies tuned to customers application		●
Metrics & alerts		●
Mitigation reports		●
Mitigation flow logs		●
DDoS rapid response support		●

Figure 19 - Azure DDoS Protection (Basic vs Standard)[16]

4.2.9.1 Recommended Security Baseline Best Practices for DDoS Protection

- Use Microsoft Defender for Cloud to enable threat protection for your DDoS Protection (Standard) resources (additional detail can be found here)
- Forward DDoS Protection logs from Azure to your SIEM platform (additional details can be found here)
- Log retention should be set for storage accounts or Log Analytics workspaces that store DDoS Protection (Standard) logs

[16] https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

- Document connectivity models between applications and flows via service endpoints that are exposed to public internet
- Have visibility on the baseline of typical traffic volumes
- Ensure that an application or system is resilient enough to handle a denial of service
- Reduce attack surface area by restricting access to required IP addresses and listening ports

Complete list of security baseline guidance from Azure Security Benchmark v2.0 for Azure DDoS Protection (Standard) can be found here.

4.2.10 Azure Network Watcher

Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs resources in a VNet. It is mainly designed for monitoring and repairing the network health issues of IaaS products (e.g., VMs, VNets, Application Gateways, Load balancers etc.). Some of the common tasks it can help with include:

- Diagnosing VM network traffic filter problems
- Diagnosing VM routing problems
- Diagnose VM outbound communication problem
- Diagnose NSG logs and traffic filtering
- Troubleshoot VPN connectivity issues

4.2.10.1 Recommended Security Baseline Best Practices for Azure Network Watcher

- Assign RBAC permissions to the user account to use Network Watcher capabilities (additional details can be found here)
- Forward logs from Network Watcher to your SIEM platform for threat detection
- Forward NSG flow logs to Azure Monitor and then use Traffic Analytics to provide insights
- Use Azure Activity Log to monitor configurations and detect changes for your Network Watcher instances
- Using Azure Policy, define and implement standard security configurations for Network Watcher (additional details can be found here)

Additional details for Network Watcher security baseline can be found here

4.2.11 Azure Bastion Hosts

Azure Bastion is a fully managed (PaaS) service that provides a secure RDP and SSH access over TLS to VMs without any exposure through public IP addresses. There is no requirement for additional software agent or public IP address on your VMs. It protects your VMs from exposing RDP/SSH ports to the outside world whilst still providing secure RDP/SSH access. As it is a fully managed service, Bastion hosts are hardened internally and hence you do not need to apply any NSGs to the Bastion subnet. If you decide to apply NSGs, then follow the details here as specific ports are required.

Additional details for security baseline can be found here
Figure 20 – Azure Bastion Host illustrates RDP/SSH connection from a Bastion host to VMs in different VNets.

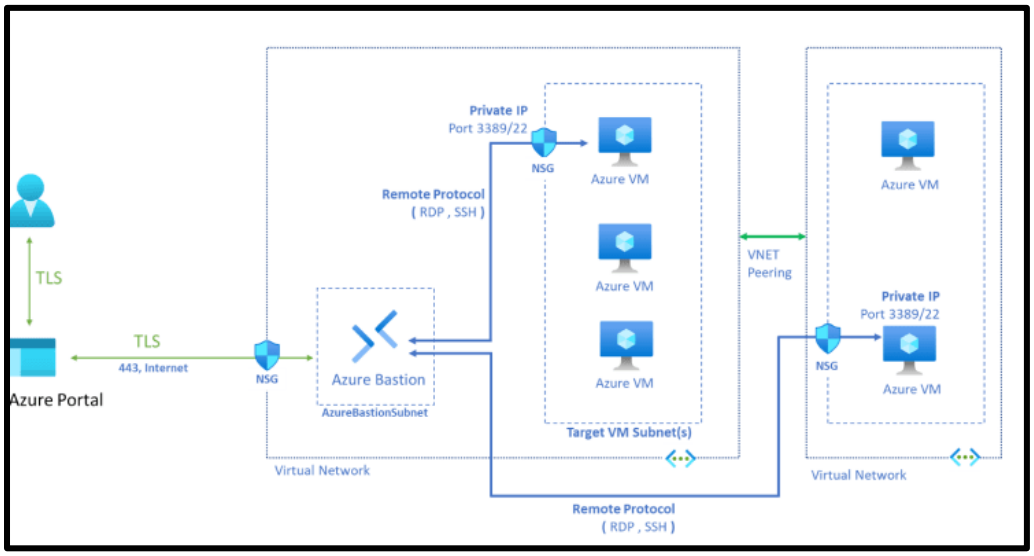

Figure 20 – Azure Bastion Host[17]

4.2.11.1 Recommended Security Baseline Best Practices for Bastion

- Use VNets to deploy Azure Bastion
- For ingress traffic from public internet, the Bastion public IP will need port 443 enabled (additional details can be found here)
- For ingress traffic from Azure Bastion control plane, enable port 443 inbound from GatewayManager service tag (additional details can be found here)
- Egress traffic to target virtual machines (VMs), NSGs will need to allow egress traffic to other VM subnets for port 3389 and 22 (additional details can be found here)
- For egress traffic to other public endpoints in Azure, enable outbound 443 to AzureCloud service tag (additional details can be found here)
- Review and reconcile user access regularly (additional details can be found here)

Additional Security baseline best practices for Azure Bastion can be found here

4.2.12 Azure Monitor

Azure Monitor is a comprehensive solution for collecting, analyzing, and acting on telemetry from cloud and on-premises environments. It helps keep control over the availability and performance of your applications and services. Some of the key functions and capabilities include:

- Detect and diagnose issues across applications and dependencies using Application Insights
- Correlate infrastructure issues using VM insights and Container insights
- Troubleshooting and deep diagnostics using Log Analytics
- Support operations at scale using Smart Alerts and Automated Actions
- Create visualization using Dashboards and Workbooks
- Collect data from monitored resources using Azure Monitor Metrics

[17] https://azure.microsoft.com/en-gb/services/azure-bastion/#features

Figure 21 – Azure Monitor gives a high-level overview including key components like two types of data stores (logs and metrics), sources of monitoring data and different functions that Azure Monitor performs with the collected data.

4.2.12.1 Recommended Security Baseline Best Practices for Azure Monitor

- Create or use existing VNet to deploy Azure Monitor resources
- Use NSGs to protect traffic flows and use service tags to define these rules (additional details can be found here)
- Configure Azure Monitor to use TLS 1.2
- Machines without internet access should use log analytics gateway to communicate with Log Analytics workspace and Azure Automation (additional details can be found here)
- Enable private link to allow access to Azure SaaS services like Azure Monitor and Azure hosted customer/partner services (additional details can be found here)
- Use managed identities for Azure Monitor resources (additional details can be found here)

Additional details on how log data security is maintained by Azure monitor can be found here and security baseline information can be found here.

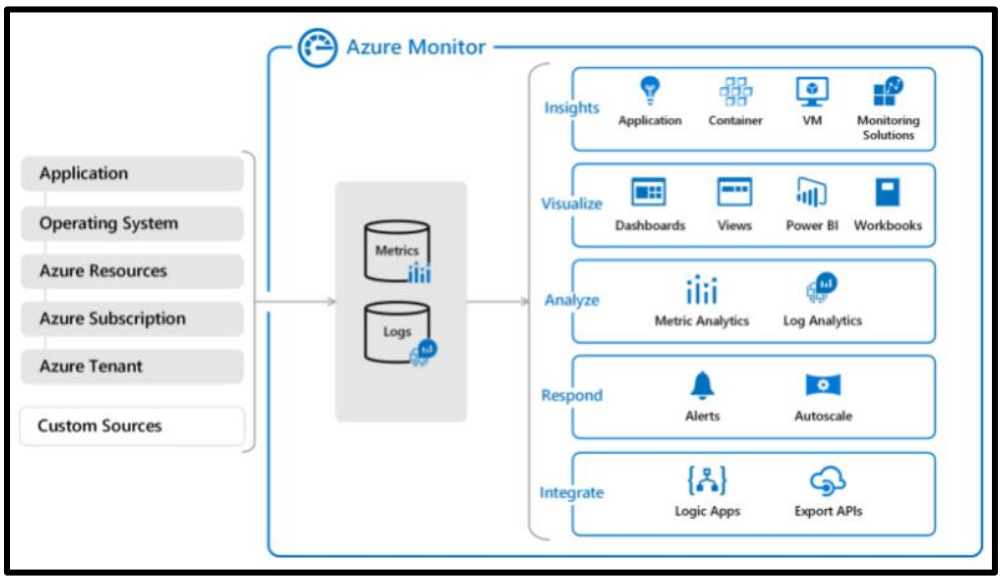

Figure 21 – Azure Monitor[18]

4.3 Azure Deployment Guidance – Automation & Orchestration

As recommended in this guide, it is a security best practice to avoid manual configurations where possible, and automated tools should be used for workload and service deployments. Whereas automated tools can help to automate tasks and resource provisioning, orchestration tools are used to deploy end-to-end workflows.

Using these tools, you can standardize the repeatable tasks and integrate security controls ensuring secure deployment of your solution in the cloud.

[18] https://docs.microsoft.com/en-us/azure/azure-monitor/overview

Azure offers various native tools that can be leveraged to deploy and manage resources, respond, and resolve issues, and orchestrate and integrate automation with other Azure or third-party services. Table 3 – Azure Automation & Orchestration Services lists key services and respective implementation guidance.

Azure Automation & Orchestration Services	Implementation Guidance
Azure Automation	Azure Automation - Quick Start Azure Automation - How-to Guide
Azure Resource Manager (ARM) templates	ARM - Quick Start ARM - How-to Guide
Azure Pipelines	Azure Pipelines - Quick Start Azure Pipelines - How-to Guide
Azure Blueprints	Azure Blueprints - Quick Start Azure Blueprints - How-to Guide

Table 3 - Azure Automation & Orchestration Services

4.3.1 Azure Automation

Azure Automation provides with a cloud-based automation, OS updates and configuration service services that supports consistent management across your Azure and non-Azure environments. It includes process automation, configuration management, update management, shared capabilities, and heterogeneous features. Figure 22 – Azure Automation illustrates the Azure Automation capabilities and key components.

Process Automation
Process Automation allows you to automate frequent, time-consuming, and manual error-prone management tasks. It allows you author graphical, PowerShell and Python runbooks. You need to deploy hybrid runbook worker to the machine or resources that are your target to run the runbooks on.

Process Automation operating environment is detailed here
Different types of automation runbooks can be found here
Details for Hybrid Runbook Worker are here

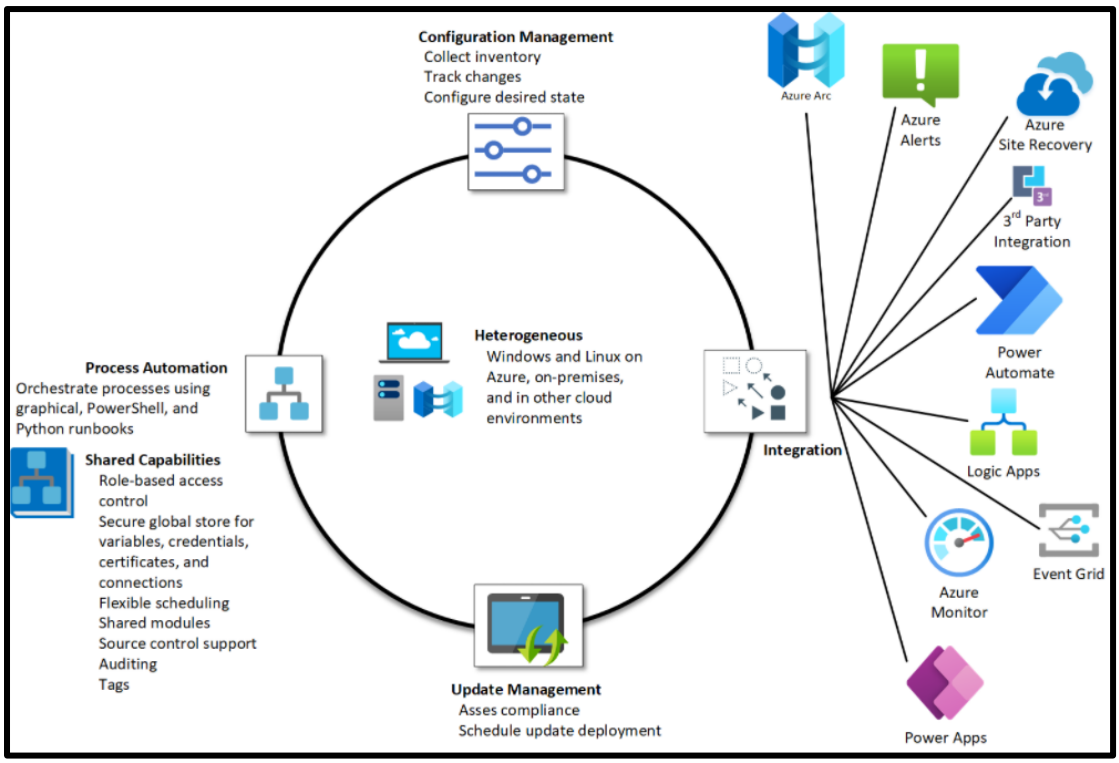

Figure 22 – Azure Automation[19]

Configuration Management
Configuration management is supported by two capabilities:

- Change Tracking and Inventory - allows you to track VMs (Windows and Linux) and server infrastructure changes. Inventory support allows you to query in-guest resources for visibility into installed applications and other configuration items. Additional details can be found here
- Azure Automation State Configuration – is a cloud-based feature for PowerShell desired state configuration (DSC) that provides services for enterprise environments. It can be used to manage DSC resources in Azure Automation and apply config to VMs or physical machines. Additional details can be found here

Update Management
Update Management gives you visibility into update compliance across Azure and other clouds, and on-premises. It lets you create scheduled deployments that orchestrate the installation of updates within a defined maintenance window. It can also be used to exclude any updates that is not applicable to a specific machine(s).

Figure 23 – Update Management illustrates how Update Management assesses and applies security updates to all connected Windows and Linux servers. Additional details can be found here

[19] https://docs.microsoft.com/en-us/azure/automation/overview

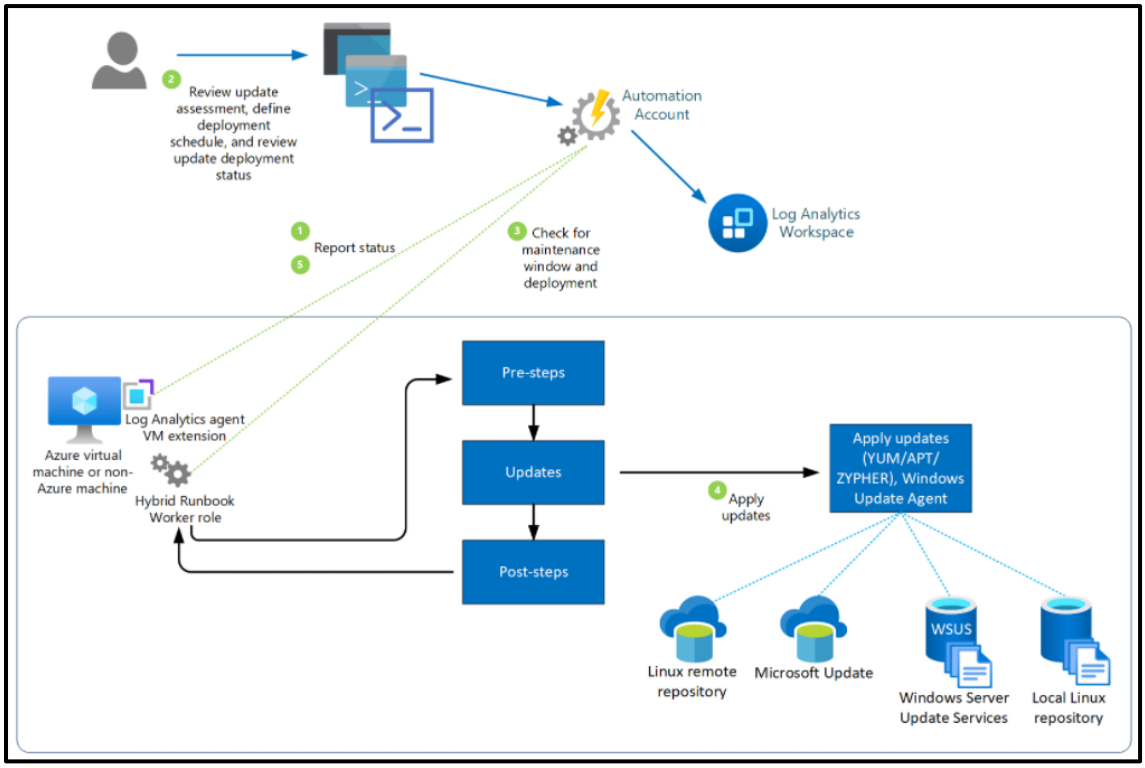

Figure 23 – Update Management[20]

Shared Capabilities

Azure Automation provides several shared capabilities, including shared resources, role-based access control, flexible scheduling, source control integration, auditing and tagging. Additional details can be found here

Heterogeneous Support (Windows and Linux)

Azure Automation is designed to work across physical servers and VMs on-premises as well as in cloud. With functionalities like Hybrid Runbook Worker (allowing runbook execution directly on the machines) and Arc-enabled servers it provides a consistent deployment and management experience for non-Azure machines. Additional details can be found here

Azure Automation - Security Considerations

Security is critical consideration especially when using automation capabilities as these features have ability to make changes at scale, and without proper controls in place this could potentially lead to security incidents.

4.3.1.1 Recommended Security Baseline Best Practices for Azure Automation

- Automation account variables should be encrypted
- Azure Automation accounts should use customer-managed keys to encrypt data at rest
- Use Azure ExpressRoute or Azure VPN to create private connections between Azure datacenters and on-premises infrastructure (additional details for ExpressRoute can be found here and Azure VPN here)

[20] https://docs.microsoft.com/en-us/azure/automation/update-management/overview

- Establish private network access to Azure services to enable private access to automation from your virtual networks without crossing the internet using Azure Private Link (additional details can be found here)
- Simplify network security rules using service tags (additional details can be found here)
- Use Azure AD for authentication and identity management of resources required for automation (additional details can be found here)
- Use X.509 self-signed certificates to authenticate Automation hybrid workers and desired state configuration (DSC) nodes to Azure Automation
- Eliminate unintended credential exposure – use scanning tools to discover credentials from the automation resources and move them to Azure Key Vault where applicable (additional details can be found here and here)
- Review and reconcile user access regularly (additional details can be found here)
- Follow the least privilege principle of just enough administration – Azure Automaton integrates with Azure RBAC to manage its resources (additional details can be found here)
- Monitor assets for risks via Microsoft Defender for Cloud (additional details can be found here)
- Use Azure Policy to audit and restrict which services users can provision in your environment (additional details can be found here)
- Enable threat detection for IAM – integrate Azure AD logs with Azure Monitor, Azure Sentinel or any other SIEM platform for monitoring and alerting (additional details can be found here)
- Enable logging for Azure resources and network activities (additional details can be found here)
- Establish secure configurations for Azure services - use Azure Blueprints to automate deployment and configuration of services and application environments (additional details can be found here)
- Conduct regular attack simulation – penetration testing or red team activities

Additional details for the applicable security baseline can be found here and data security can be found here.

4.3.2 Azure Resource Manager (ARM) templates

Azure Resource Manager is the deployment and management service. It enables you to create, update and delete resources in your Azure account. Features like access control, locks, and tags are used to secure and organize resources after deployment. Figure 24 – Azure Resource Manager shows the role it plays in handling Azure functionalities.

Resource manager can help to manage your infrastructure through templates and scripts, can manage the resources collectively as group hence reducing the admin overhead, use of templates and scripts ensures resources are deployed in a consistent state, define dependencies between resource, apply access control to all services via RBAC and manage and organize your resources using tags. Additional details can be found here.

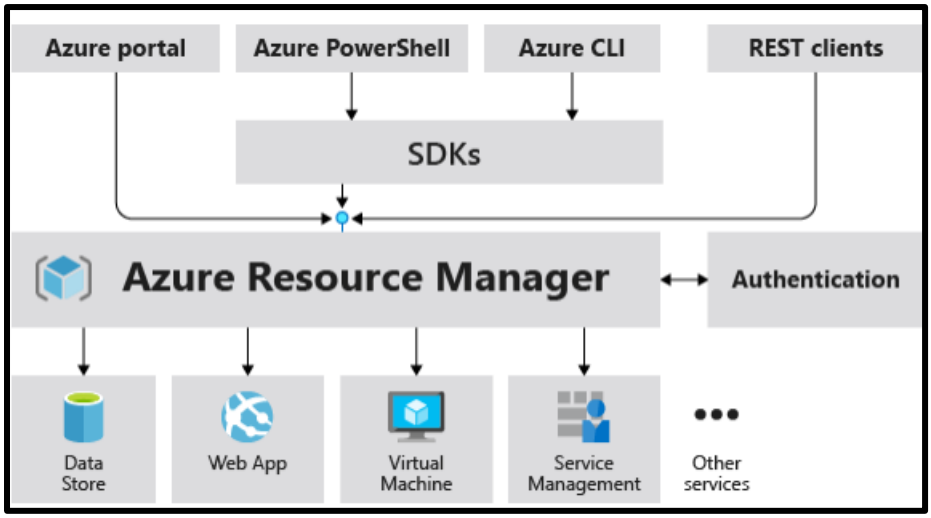

Figure 24 – Azure Resource Manager[21]

4.3.2.1 Recommended Security Baseline Best Practices for ARM

Below are some best practices security guidance which should be considered when ARM is used:

- Use TLS v1.2 or higher version while connecting to Azure Resource manager (additional details can be found here)
- Use Azure Private Link to enable private access to Azure Resource Manager from your virtual networks without crossing the internet (additional details can be found here)
- Use Azure Virtual Network service tags to define network access controls for Azure Resource Manager resources on network security groups or Azure Firewall (additional details can be found here)
- Implement Credential Scanner for your repositories hosting ARM templates - this will help you identify and prevent credentials within your code (additional details can be found here and here)
- Review and reconcile user access regularly
- Follow the least privilege principle of just enough administration – ARM integrates with Azure RBAC to manage its resources (additional details can be found here)
- Enable MFA for accounts on your subscription
- Maximum of three owners should be designated for your subscription
- External accounts with owner permissions should be removed from your subscription
- Enable threat detection for IAM – integrate Azure AD logs with Azure Monitor, Azure Sentinel or any other SIEM platform for monitoring and alerting (additional details can be found here)
- Enable logging for Azure resources and network activities (additional details can be found here and here)
- Conduct regular attack simulation – penetration testing or red team activities
- Azure defender should be enabled for relevant services in use in your subscription
- High severity alerts should have email notification to the subscription owner enabled.

Additional details for Azure ARM security baseline can be found here

[21] https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview

4.3.3 Azure Pipelines

Azure Pipelines automatically builds and tests code projects to make them available to others. It supports majority of languages and code types. It combines continuous integration (CI) and continuous delivery (CD) to test and build your code and ship it to any target. CI is the practice used by developments teams to automate merging and testing code whereas CD is a process used to build code, test it, and deploy it to one or more test and production environments. Continuous testing (CT) is the use of automated build-deploy-test workflows with a choice of technologies and frameworks, which test your changes continuously in a fast, scalable, and efficient manner.

Azure Pipelines provides a quick, easy, and safe way to automate building your projects and making them available to the users. You can use YAML pipeline editor to build pipelines as shown in Figure 25 – Azure Pipeline using YAML editor.

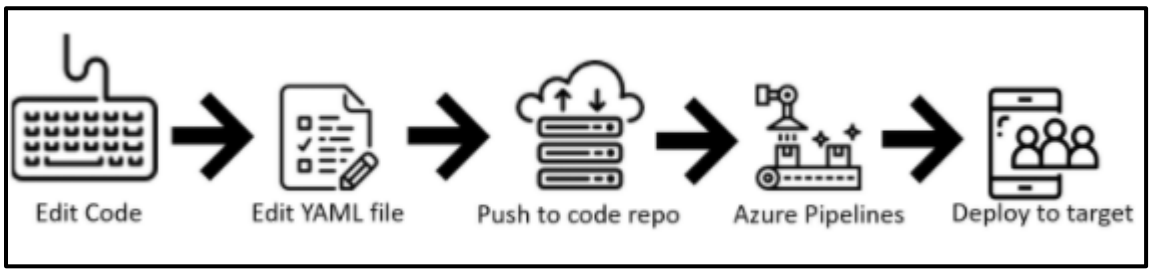

Figure 25 - Azure Pipeline using YAML[22]

Basic steps are:

1. Configure Azure Pipelines to use your Git repo
2. Edit your azure-pipelines.yml file to define your build
3. Push your code to your version control repository. This action kicks off the default trigger to build and deploy and then monitor the results

Alternatively, classic interface can also be used to define pipelines – see Figure 26 - Azure Pipelines using classic interface.

Basic steps include:

1. Configure Azure Pipelines to use your Git repo
2. Use the Azure Pipelines classic editor to create and configure your build and release pipelines
3. Push your code to your version control repository. This action triggers your pipeline and runs tasks such as building or testing code

[22] https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started/pipelines-get-started?view=azure-devops

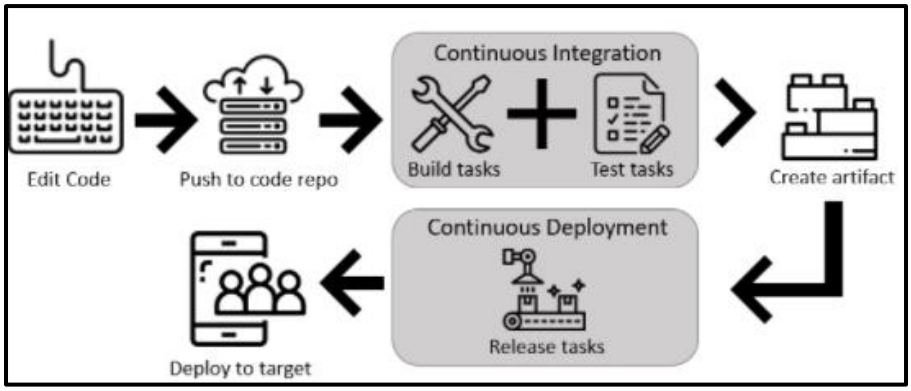

Figure 26 – Azure Pipelines using classic interface[22]

4.3.3.1 Recommended Security Baseline Best Practices for Azure Pipelines

You can run scripts or deploy code to production environments using pipelines, but you need to make sure that these pipelines are not used to deploy malicious code and ensure that only intended code is deployed. Hence security for pipelines could bring in new unique challenges which should be considered. Below are some key considerations:

- Permissions and branch policies must be employed to ensure changes to the code and pipeline are safe
- Add a repository resource check to protect your repository resource (additional details can be found here)
- Review default repository permissions (more details are here)
- Do not provide secrets to fork builds
- Consider manually triggering fork builds
- Use Microsoft-hosted agents for fork builds
- Understand Azure Repo permissions model to ensure user branches are created by authorized personnel only
- Consider managing each product and team in a separate project, this will prevent lateral exposure
- Start with “extends” templates which will provide an outer structure hence preventing malicious code from getting into your pipeline
- Restrict what services the Azure Pipelines agent will provide to user steps
- Restrict stages and jobs to run under specific conditions
- Where applicable make the variables in use read-only
- Use Microsoft-hosted pools instead of self-hosted pools – this will offer isolation and clean VM for each pipeline

Additional details for Azure Pipelines can be found here

[22] https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started/pipelines-get-started?view=azure-devops

4.3.4 Azure Blueprints

Azure Blueprints enables you to define repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Blueprints are a declarative way to orchestrate the deployment of various resource templates and artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager (ARM) templates
- Resource Groups

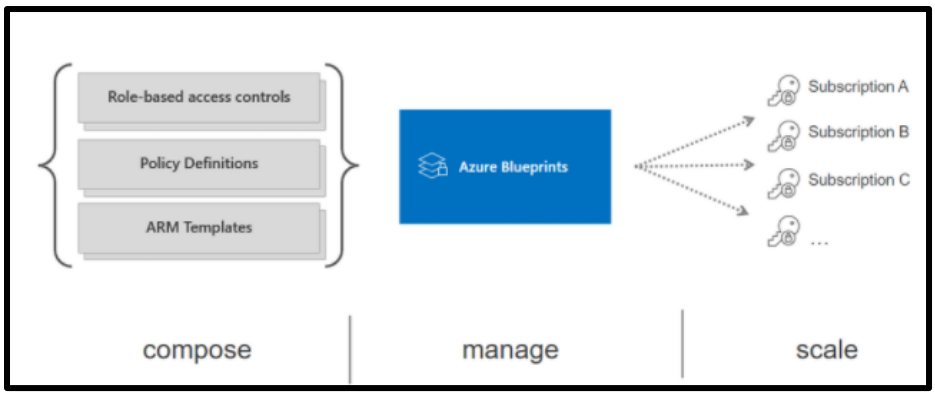

Figure 27 – Azure Blueprints[23]

Blueprint packages these templates and artifacts and allows you to version these packages (including using a CI/CD pipeline). Each package is assigned to subscription(s) in a single operation which can be audited and tracked.

High-level blueprint deployment steps:

1. Azure blueprints granted owners' rights
2. The blueprints assignment object is created
3. Azure Blueprints creates system-assigned managed identity
4. The managed identity deploys blueprint artifacts
5. Azure blueprints service and system-assigned managed identity rights are revoked

Unlike ARM templates that are only used for deployment and do not preserve any relationships with deployed resources, Azure Blueprints preserve these relationships, support improved tracking and auditing of deployments and ability to upgrade subscriptions governed by the same blueprint.

Additional details on Azure Blueprints can be found here
GitHub Azure Blueprints samples can be found here
Azure Blueprints Compliance samples can be found here

[23] https://techcommunity.microsoft.com/t5/itops-talk-blog/azure-blueprints-vs-azure-resource-manager-template-specs/ba-p/2176909

4.4 Azure Security Best Practices & Guidance

Microsoft recommend a number of key security best practices to facilitate secure deployments of media related workloads into Azure. The table below summarizes these and provides useful details of which Azure services are required along with links to the relevant Microsoft configuration guidance. Convergent recommends using these Microsoft Azure recommended best practices as a checklist to ensure all best practices are considered. It should be noted that these best practices are further mapped to various standards and frameworks that are applicable to the media and entertainment industry (see Appendix A)

4.4.1 Optimize Identity & Access Management

Azure Security Best Practice	**Treat identity as the primary security perimeter**
Background	
Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security. Network perimeters keep getting more porous, and that perimeter defense cannot be as effective as it was before the explosion of BYOD devices and cloud applications. Azure Active Directory (Azure AD) is the Azure solution for identity and access management. Azure AD is a multitenant, cloud-based directory and identity management service from Microsoft. It combines core directory services, application access management, and identity protection into a single solution.	
Microsoft Guidance	**Azure Service Enabling**
Leverage Azure AD for identity and access management. Azure AD is a multitenant, cloud-based directory and identity management service from Microsoft. It combines core directory services, application access, and advanced identity protection. For more information, see: Azure AD Premium Azure AD Identity Protection	Azure AD Premium Azure AD Identity Protection

Azure Security Best Practice	**Centralize identity management**
Background	
In a hybrid identity scenario, we recommend that you integrate your on-premises and cloud directories. Integration enables your IT team to manage accounts from one location, regardless of where an account is created. Integration also helps your users be more productive by providing a common identity for accessing both cloud and on-premises resources.	
Microsoft Guidance	**Azure Service Enabling**
Establish a single Azure AD instance. Consistency and a single authoritative source will increase clarity and reduce security risks from human errors and configuration complexity. For more information, see: Azure AD Fundamentals	Azure AD
Integrate your on-premises directories with Azure AD by using AD connect to synchronize your on-premises directory with your cloud directory. For more information, see: Azure AD Connect	Azure AD Connect
Do not synchronize accounts to Azure AD that have high privileges in your existing AD instance. (The default AD Connect configuration filters out these accounts)	Azure AD Connect

This approach mitigates the risk of a malicious actor pivoting from cloud to on-premises assets (or vice-versa) which could cause a major incident. For more information, see: Azure AD Connect	

Turn on password hash synchronization. Password hash synchronization is a feature used to sync user password hashes from an on-premises Active Directory instance to a cloud-based Azure AD instance. This sync helps to protect against leaked credentials being replayed from previous attacks. Even if you decide to use federation with Active Directory Federation Services (AD FS) or other identity providers, you can optionally set up password hash synchronization as a backup in case your on-premises servers fail or become temporarily unavailable. This sync enables users to sign-in to the service by using the same password that they use to sign in to their on-premises Active Directory instance. It also allows Identity Protection to detect compromised credentials by comparing synchronized password hashes with passwords known to be compromised, if a user has used the same email address and password on other services that are not connected to Azure AD. For more information, see: Password Hash synchronization	Azure AD Connect
For new application development, use Azure AD for authentication. Use the correct capabilities to support authentication: - Azure AD for employees - Azure AD B2B for guest users and external partners - Azure AD B2C to control how customers sign up, sign in, and manage their profiles when they use your applications. For more information, see: Azure AD External Identities Azure AD B2C	Azure AD B2B & B2C

Azure Security Best Practice	**Manage Connected Tenants**
Background	
Your security organization needs visibility to assess risk and to determine whether the policies of your organization, and any regulatory requirements, are being followed. You should ensure that your security organization has visibility into all subscriptions connected to your production environment and network (via Azure ExpressRoute or site-to-site VPN). A Global Administrator/Company Administrator in Azure AD can elevate their access to the User Access Administrator role and see all subscriptions and managed groups connected to your environment.	
Microsoft Guidance	**Azure Service Enabling**
Leverage "elevate access" to manage all Azure subscriptions and management groups to ensure that you and your security group can view all subscriptions or management groups connected to your environment. You should remove this elevated access after you have assessed risks. For more information, see: Elevate Access Global Admin Azure ExpressRoute VPN Gateway Multi-Site-to-Site Azure AD Built-in Roles Azure AD Built-in Roles - User Access Admin	Azure AD

Azure Security Best Practice	Enable Single-Sign-On
Background	
In a mobile-first, cloud-first world, you want to enable single sign-on (SSO) to devices, apps, and services from anywhere so your users can be productive wherever and whenever. When you have multiple identity solutions to manage, this becomes an administrative problem not only for IT but also for users who have to remember multiple passwords. By using the same identity solution for all your apps and resources, you can achieve SSO. In addition, your users can leverage the same set of credentials to sign in and access the resources that they need, whether the resources are located on-premises or in the cloud. Organizations that don't create a common identity to establish SSO for their users and applications are more exposed to scenarios where users have multiple passwords. These scenarios increase the likelihood of users reusing passwords or using weak passwords.	
Microsoft Guidance	**Azure Service Enabling**
Enable Azure SSO For more information, see: Azure Single-Sign-On	Azure AD

Azure Security Best Practice	Turn on conditional access
Background	
Users can access your organization's resources by using a variety of devices and apps from anywhere. As an IT admin, you want to make sure that these devices meet your standards for security and compliance. Just focusing on who can access a resource is not sufficient anymore. To balance security and productivity, you need to think about how a resource is accessed before you can make a decision about access control. With Azure AD conditional access, you can address this requirement. With conditional access, you can make automated access control decisions—based on conditions—for accessing your cloud apps.	
Microsoft Guidance	**Azure Service Enabling**
Manage and control access to corporate resources. Configure Azure AD conditional access based on a group, location, and application sensitivity for SaaS apps and Azure AD–connected apps. For more information, see: Azure AD Conditional Access	Azure AD Conditional Access
Block legacy authentication protocols. Attackers exploit weaknesses in older protocols every day, particularly for password spray attacks. Configure conditional access to block legacy protocols. For more information, see: Azure AD Best Practices - Video	Azure AD Conditional Access

Azure Security Best Practice	Enable Password Management
Background	
If you have multiple tenants or want to enable users to reset their own passwords, it's important that you use appropriate security policies to prevent abuse. Enhance password policies in your organization by performing the same checks for on-premises password changes as you do for cloud-based password changes. Install Azure AD password protection for Windows Server Active Directory agents on-premises to extend banned password lists to your existing infrastructure. Users and admins who change, set, or reset passwords on-premises are required to comply with the same password policy as cloud-only users.	
Microsoft Guidance	**Azure Service Enabling**
- Set up self-service password reset (SSPR) for your users. **- Monitor how or if SSPR is really being used by leveraging the "Azure AD Password Reset Registration Activity Report"** For more information, see: Azure AD Password Management Reporting Azure AD Password Protection	Azure AD SSPR Azure AD Password Protection
Extend cloud-based password policies to your on-premises infrastructure. For more information, see: Azure AD Password Protection	Azure AD SSPR Azure AD Password Protection
Option 1 - Enable MFA by on a per user account basis. **(Not recommended as this can result in unintentional MFA exceptions)** For more information, see: Enable MFA per user	Azure AD
Option 2- Enable MFA with a Conditional Access Policy. **(Recommended)** Users are prompted for two-step verification under specific conditions such as untrusted locations or devices that you consider risky. For more information, see: Azure AD MFA Azure AD Conditional Access	Azure AD (Premium)
Option 3 - Enable MFA with a Conditional Access Policy and evaluate sign-on risk with Azure AD Identity protection **(Recommended)** This option enables you to: - Detect potential vulnerabilities that affect your organization's identities. - Configure automated responses to detected suspicious actions that are related to your organization's identities. - Investigate suspicious incidents and take appropriate action to resolve them. This method uses the Azure AD Identity Protection risk evaluation to determine if two- step verification is required based on user and sign-in risk for all cloud applications. For more information, see: Azure AD MFA Azure AD Conditional Access Azure AD Identity Protection	Azure AD (P2) Azure Identity Protection

Azure Security Best Practice	Use Role Based Access Control

Background

Access management for cloud resources is critical for any organization that uses the cloud. Role- based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.
Designating groups or individual roles responsible for specific functions in Azure helps avoid confusion that can lead to human and automation errors that create security risks. Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.
Your security team needs visibility into your Azure resources to assess and remediate risk. If the security team has operational responsibilities, they need additional permissions to do their jobs.
You can use RBAC to assign permissions to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource.

Microsoft Guidance	Azure Service Enabling
Segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, allow only certain actions at a particular scope. Use built-in RBAC roles in Azure to assign privileges to users. Note: Specific permissions create unneeded complexity and confusion, accumulating into a "legacy" configuration that's difficult to fix without fear of breaking something. - Avoid resource-specific permissions. Instead, use management groups for enterprise-wide permissions and resource groups for permissions within subscriptions. - Avoid user-specific permissions. Instead, assign access to groups in Azure AD.	Azure AD
Grant security teams with Azure responsibilities access to see Azure resources so they can assess and remediate risk. **Grant security teams the RBAC Security Reader role. You can use the root management group or the segment management group, depending on the scope of responsibilities:** • Root management group for teams responsible for all enterprise resources • Segment management group for teams with limited scope (commonly because of regulatory or other organizational boundaries) For more information, see: RBAC Security Reader Role	Azure AD
Grant the appropriate permissions to security teams that have direct operational responsibilities. Review the RBAC built-in roles for the appropriate role assignment. If the built-in roles don't meet the specific needs of your organization, you can create custom roles for Azure resources. As with built-in roles, you can assign custom roles to users, groups, and service principals at subscription, resource group, and resource scopes. For more information, see: RBAC - Custom Roles	Azure AD
Grant Microsoft Defender for Cloud access to security roles that need it. Microsoft Defender for Cloud allows security teams to quickly identify and remediate risks. Add security teams with these needs to the RBAC Security Admin role so they can view security policies, view security states, edit security policies, view alerts and recommendations, and dismiss alerts and recommendations. You can do this by using the root management group or the segment management group, depending on the scope of responsibilities. For more information, see: RBAC - Security Admin	Azure AD

Azure Security Best Practice	Lower Exposure of Privileged Accounts
Background	
Securing privileged access is a critical first step to protecting business assets. Minimizing the number of people who have access to secure information or resources reduces the chance of a malicious user getting access, or an authorized user inadvertently affecting a sensitive resource. Privileged accounts are accounts that administer and manage IT systems. Cyber attackers target these accounts to gain access to an organization's data and systems. To secure privileged access, you should isolate the accounts and systems from the risk of being exposed to a malicious user.	
Microsoft Guidance	**Azure Service Enabling**
Manage, control, and monitor access to privileged accounts. Turn on Azure AD Privileged Identity Management. After you turn on Privileged Identity Management, you will receive notification email messages for privileged access role changes. These notifications provide early warning when additional users are added to highly privileged roles in your directory. For more information, see: Security Privileged Access	Azure AD Privileged Identity Management
Ensure all critical admin accounts are managed Azure AD accounts. Remove any consumer accounts from critical admin roles (for example, Microsoft accounts like @hotmail.com, @live.com, and @outlook.com). For more information, see: Azure AD	Azure AD
Ensure all critical admin roles have a separate account for administrative tasks to avoid phishing and other attacks to compromise administrative privileges. Create a separate admin account that is assigned the privileges needed to perform the administrative tasks. Block the use of these administrative accounts for daily productivity tools like Microsoft Office 365 email or arbitrary web browsing. For more information, see: Azure AD	Azure AD
Identify and categorize accounts that are in highly privileged roles. After turning on Azure AD Privileged Identity Management, view the users who are in the global administrator, privileged role administrator, and other highly privileged roles. Remove any accounts that are no longer needed in those roles, and categorize the remaining accounts that are assigned to admin roles: - Individually assigned to administrative users, and can be used for non-administrative purposes (for example, personal email) - Individually assigned to administrative users and designated for administrative purposes only - Shared across multiple users - For emergency access scenarios - For automated scripts - For external users For more information, see: Azure AD Privileged Identity Management	Azure AD Privileged Identity Management
Implement "just-in-time" (JIT) access to further lower the exposure time of privileges and increase your visibility into the use of privileged accounts. Azure AD Privileged Identity Management lets you: - Limit users to only taking on their privileges JIT. - Assign roles for a shortened duration with confidence that the privileges are revoked automatically.	Azure AD Privileged Identity Management

For more information, see: Azure AD Privileged Identity Management	
Define at least two emergency access accounts. Emergency access accounts help organizations restrict privileged access in an existing Azure Active Directory environment. These accounts are highly privileged and are not assigned to specific individuals. Emergency access accounts are limited to scenarios where normal administrative accounts cannot be used. Organizations must limit the emergency account's usage to only the necessary amount of time. Evaluate the accounts that are assigned or eligible for the global admin role. If you do not see any cloud-only accounts by using the *.onmicrosoft.com domain (intended for emergency access), create them. For more information, see: Azure AD - Manage Emergency Access	Azure Active Directory
Have a “break glass" process in place in case of an emergency. For more information, see: Azure AD - Secure Admin Roles	Azure Active Directory
Require all critical admin accounts to be password-less (preferred) or require Multi-Factor Authentication. Use the Microsoft Authenticator app to sign into any Azure AD account without using a password. Like Windows Hello for Business, the Microsoft Authenticator uses key-based authentication to enable a user credential that’s tied to a device and uses biometric authentication or a PIN. Require Azure Multi-Factor Authentication at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles: Global Administrator, Privileged Role Administrator, Exchange Online Administrator, and SharePoint Online Administrator. Enable Multi-Factor Authentication for your admin accounts and ensure that admin account users have registered. For more information, see: Microsoft Authentication App Enable per user MFA MFA Setup	Azure AD MS Authenticator App
For critical admin accounts, have an admin workstation where production tasks are not allowed (for example, browsing and email). This will protect your admin accounts from attack vectors that use browsing and email and significantly lower your risk of a major incident. Use an admin workstation. Choose a level of workstation security: - Highly secure productivity devices provide advanced security for browsing and other productivity tasks. - Privileged Access Workstations (PAWs) provide a dedicated operating system that is protected from internet attacks and threat vectors for sensitive tasks. For more information, see: Secured-core PC Privileged Access Workstations	N/A
Deprovision admin accounts when employees leave your organization. Have a process in place that disables or deletes admin accounts when employees leave your organization.	N/A
Regularly test admin accounts by using current attack techniques. Use Defender for Office 365 Attack Simulator or a third-party offering to run realistic attack scenarios in your organization. This can help you find vulnerable users before a real attack occurs.	Defender for O365 Attack Simulator

For more information, see: Defender for O365 Attack Simulator	
Take steps to mitigate the most frequently used attacked techniques in line with the following best practices: • Identify Microsoft accounts in administrative roles that need to be switched to work accounts. • Ensure separate user accounts and mail forwarding for global administrator accounts. • Ensure that the passwords of administrative accounts have recently changed. • Turn on password hash synchronization. • Require Multi-Factor Authentication for users in all privileged roles as well as exposed users. • Obtain your Office 365 Secure Score (if using Office 365). • Review the Office 365 security and compliance guidance (if using Office 365) • Configure Office 365 Activity Monitoring (if using Office 365). • Establish incident/emergency response plan owners. • Secure on-premises privileged administrative accounts. Links for the above: Role Security Planning Azure AD - Secure Admin Roles Turn on password hash synchronization Require MFA for users in all privileged roles Obtain your office 365 secure score if using office 365 Review the office 365 security and compliance guidance if using office 365 Configure office 365 activity monitoring if using office 365 Establish incident emergency response plan owners Secure on premises privileged administrative accounts if not already done	Azure AD O365 Activity Monitoring

Azure Security Best Practice	**Control locations where resources are created**
Background	
Enabling cloud operators to perform tasks while preventing them from breaking conventions that are needed to manage your organization's resources is very important. Organizations that want to control the locations where resources are created should hard code these locations. Organizations that are not controlling how resources are created are more susceptible to users who might abuse the service by creating more resources than they need. Hardening the resource creation process is an important step to securing a multitenant scenario.	
Microsoft Guidance	**Azure Service Enabling**
Use Azure Resource Manager to create security policies whose definitions describe the actions or resources that are specifically denied. You assign those policy definitions at the desired scope, such as the subscription, the resource group, or an individual resource. Note: Security policies are not the same as RBAC. They actually use RBAC to authorize users to create those resources. For more information, see: Azure Resource Manager	Azure Resource Manager

Azure Security Best Practice	Actively monitor for suspicious activities
Background	
An active identity monitoring system can quickly detect suspicious behavior and trigger an alert for further investigation.	
Microsoft Guidance	**Azure Service Enabling**
Leverage Azure AD premium anomaly reports to identify suspicious user account activity Have a method to identify: - Attempts to sign in without being traced. - Brute force attacks against a particular account. - Attempts to sign in from multiple locations. - Sign-ins from infected devices. - Suspicious IP addresses. Use Azure AD Premium anomaly reports. Have processes and procedures in place for IT admins to run these reports on a daily basis or on demand (usually in an incident response scenario). For more information, see: AD View access usage reports Reports monitoring - how to find activity reports	Azure AD Premium Azure AD Identity Protection
Have an active monitoring system that notifies you of risks and can adjust risk level (high, medium, or low) to your business requirements Use Azure AD Identity Protection, which flags the current risks on its own dashboard and sends daily summary notifications via email. To help protect your organization's identities, you can configure risk-based policies that automatically respond to detected issues when a specified risk level is reached. For more information, see: Active Directory Identity Protection	Azure AD Premium Azure AD Identity Protection

Azure Security Best Practice	Use Azure AD for storage authentication
Background	
Azure Storage supports authentication and authorization with Azure AD for Blob storage and Queue storage. With Azure AD authentication, you can use Azure role-based access control to grant specific permissions to users, groups, and applications—down to the scope of an individual blob container or queue.	
Microsoft Guidance	**Azure Service Enabling**
Microsoft recommend that you use Azure AD for authenticating access to storage. For more information, see: Azure Storage - Azure Active Directory based access control	Azure AD

4.4.2 Use Strong Network Controls

Azure Security Best Practice	Logically segment subnets
Background	
Azure virtual networks are similar to LANs on your on-premises network. The idea behind an Azure virtual network is that you create a network, based on a single private IP address space, on which you can place all your Azure virtual machines. The private IP address spaces available are in the Class A (10.0.0.0/8), Class B (172.16.0.0/12), and Class C (192.168.0.0/16) ranges.	
Microsoft Guidance	**Azure Service Enabling**
Do not assign allow rules with broad ranges (for example, allow 0.0.0.0 through 255.255.255.255 Ensure troubleshooting procedures discourage or ban setting up these types of rules. These allow rules lead to a false sense of security and are frequently found and exploited by red teams. For more information, see: Virtual Network Subnet Azure Network Security Groups	Azure Network Security Groups Azure Subnets
Segment the larger address space into subnets. Use CIDR-based subnetting principles to create your subnets. For more information, see: Virtual Network Subnet Azure Network Security Groups	Azure Network Security Groups Azure Subnets
Create network access controls between subnets. Routing between subnets happens automatically, and you don't need to manually configure routing tables. By default, there are no network access controls between the subnets that you create on an Azure virtual network. Use a network security group to protect against unsolicited traffic into Azure subnets. Network security groups are simple, stateful packet inspection devices that use the 5-tuple approach (source IP, source port, destination IP, destination port, and layer 4 protocol) to create allow/deny rules for network traffic. You allow or deny traffic to and from a single IP address, to and from multiple IP addresses, or to and from entire subnets. When you use network security groups for network access control between subnets, you can put resources that belong to the same security zone or role in their own subnets. For more information, see: Azure Virtual Network Azure Network Security Groups	Azure Network Security Groups Azure Subnets
Avoid small virtual networks and subnets to ensure simplicity and flexibility. Most organizations add more resources than initially planned, and re-allocating addresses is labor intensive. Using small subnets adds limited security value and mapping a network security group to each subnet adds overhead. Define subnets broadly to ensure that you have flexibility for growth. For more information, see: Azure Virtual Network Azure Network Security Groups	Azure Network Security Groups Azure Subnets
Simplify network security group rule management by defining Application Security Groups.	Azure Network Security Groups Azure Subnets

Define an Application Security Group for lists of IP addresses that you think might change in the future or be used across many network security groups. Be sure to name Application Security Groups clearly so others can understand their content and purpose. For more information, see: Application Security Groups Azure Virtual Network Azure Network Security Groups	

Azure Security Best Practice	**Adopt a Zero Trust Approach**
Background	
Perimeter-based networks operate on the assumption that all systems within a network can be trusted. But today's employees access their organization's resources from anywhere on a variety of devices and apps, which makes perimeter security controls irrelevant. Access control policies that focus only on who can access a resource are not enough. To master the balance between security and productivity, security admins also need to factor in how a resource is being accessed. Networks need to evolve from traditional defenses because networks might be vulnerable to breaches: an attacker can compromise a single endpoint within the trusted boundary and then quickly expand a foothold across the entire network. Zero Trust networks eliminate the concept of trust based on network location within a perimeter. Instead, Zero Trust architectures use device and user trust claims to gate access to organizational data and resources. For new initiatives, adopt Zero Trust approaches that validate trust at the time of access.	
Microsoft Guidance	**Azure Service Enabling**
Simplify network security group rule management by defining Application Security Groups. Define an Application Security Group for lists of IP addresses that you think might change in the future or be used across many network security groups. Be sure to name Application Security Groups clearly so others can understand their content and purpose. For more information, see: Application Security Groups	Azure Conditional Access Azure Just-in-time access Azure Privileged Identity Management
Enable port access only after workflow approval. You can use just-in-time VM access in Azure Security Center to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. For more information, see: Just-in-time Access	Azure Conditional Access Azure Just-in-time access Azure Privileged Identity Management
Grant temporary permissions to perform privileged tasks. This prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it. Use just-in-time access in Azure AD Privileged Identity Management or in a third-party solution to grant permissions to perform privileged tasks. For more information, see: PIM Configure	Azure Conditional Access Azure Just-in-time access Azure Privileged Identity Management

Azure Security Best Practice	Control Routing Behavior
Background	
When you put a virtual machine on an Azure virtual network, the VM can connect to any other VM on the same virtual network, even if the other VMs are on different subnets. This is possible because a collection of system routes enabled by default allows this type of communication. These default routes allow VMs on the same virtual network to initiate connections with each other, and with the internet (for outbound communications to the internet only). Although the default system routes are useful for many deployment scenarios, there are times when you want to customize the routing configuration for your deployments. You can configure the next- hop address to reach specific destinations.	
Microsoft Guidance	**Azure Service Enabling**
Configure user-defined routes when you deploy a security appliance for a virtual network. For more information, see: Virtual Networks UDR Overview	Azure User Defined Routing

Azure Security Best Practice	Use virtual network appliances
Background	
Network security groups and user-defined routing can provide a certain measure of network security at the network and transport layers of the OSI model. But in some situations, you want or need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances provided by Azure partners.	
Microsoft Guidance	**Azure Service Enabling**
Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include: - Firewalling - Intrusion detection/intrusion prevention - Vulnerability management - Application control - Network-based anomaly detection - Web filtering - Antivirus - Botnet protection To find available Azure virtual network security appliances, go to the Azure Marketplace and search for “security” and “network security.” For more information, see: Azure Marketplace	Azure Marketplace

Azure Security Best Practice	Deploy perimeter networks for security zones

Background

A perimeter network (also known as a DMZ) is a physical or logical network segment that provides an additional layer of security between your assets and the internet. Specialized network access control devices on the edge of a perimeter network allow only desired traffic into your virtual network.
Perimeter networks are useful because you can focus your network access control management, monitoring, logging, and reporting on the devices at the edge of your Azure virtual network. A perimeter network is where you typically enable distributed denial of service (DDoS) prevention, intrusion detection/intrusion prevention systems (IDS/IPS), firewall rules and policies, web filtering, network antimalware, and more. The network security devices sit between the internet and your Azure virtual network and have an interface on both networks.
Although this is the basic design of a perimeter network, there are many different designs, like back- to-back, tri-homed, and multi-homed.

Microsoft Guidance	Azure Service Enabling
Based on the Zero Trust concept mentioned earlier, we recommend that you consider using a perimeter network for all high security deployments to enhance the level of network security and access control for your Azure resources. You can use Azure or a third-party solution to provide an additional layer of security between your assets and the internet: -Azure native controls. Azure Firewall and the web application firewall in Application Gateway offer basic security with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration. - Third-party offerings. Search the Azure Marketplace for next-generation firewall (NGFW) and other third-party offerings that provide familiar security tools and significantly enhanced levels of network security. Configuration might be more complex, but a third-party offering might allow you to use existing capabilities and skill sets. For more information, see: Azure Firewall Azure Virtual Networking Azure Marketplace	Azure Firewall Azure Virtual Networking Azure Marketplace

Azure Security Best Practice	Avoid exposure to the internet with dedicated WAN links

Background

Many organizations have chosen the hybrid IT route. With hybrid IT, some of the company's information assets are in Azure, and others remain on-premises. In many cases, some components of a service are running in Azure while other components remain on-premises.
In a hybrid IT scenario, there's usually some type of cross-premises connectivity. Cross-premises connectivity allows the company to connect its on-premises networks to Azure virtual networks.

Microsoft Guidance	Azure Service Enabling
Configure secure connections into Azure There are two options to achieve this: - Site-to-site VPN. It is a trusted, reliable, and established technology, but the connection takes place over the internet. Bandwidth is constrained to a maximum of about 200 Mbps. Site-to- site VPN is a desirable option in some scenarios. - Azure ExpressRoute. We recommend that you use ExpressRoute for your cross-premises connectivity. ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services like Azure, Office 365, and Dynamics 365. ExpressRoute is a dedicated WAN link between your on-premises location or a Microsoft Exchange hosting provider. Because this is a telco connection, your data does not travel over the internet, so it isn't exposed to the potential risks of internet communications.	Azure ExpressRoute Azure Site-to-Site VPN

The location of your ExpressRoute connection can affect firewall capacity, scalability, reliability, and network traffic visibility. You will need to identify where to terminate ExpressRoute in existing (on-premises) networks. You can: - Terminate outside the firewall (the perimeter network paradigm) if you require visibility into the traffic, if you need to continue an existing practice of isolating datacenters, or if you're solely putting extranet resources on Azure. - Terminate inside the firewall (the network extension paradigm). This is the default recommendation. In all other cases, we recommend treating Azure as an nth datacenter. For more information, see: Azure ExpressRoute Azure Site-to-Site VPN	

Azure Security Best Practice	**Optimize uptime and performance**
Background	
From a security perspective, you need to do whatever you can to make sure that your services have optimal uptime and performance. A popular and effective method for enhancing availability and performance is load balancing. Load balancing is a method of distributing network traffic across servers that are part of a service. For example, if you have front-end web servers as part of your service, you can use load balancing to distribute the traffic across your multiple front-end web servers. This distribution of traffic increases availability because if one of the web servers becomes unavailable, the load balancer stops sending traffic to that server and redirects it to the servers that are still online. Load balancing also helps performance, because the processor, network, and memory overhead for serving requests is distributed across all the load-balanced servers.	
Microsoft Guidance	**Azure Service Enabling**
We recommend that you employ load balancing whenever you can, and as appropriate for your services. The following scenarios at both the Azure virtual network level and the global level, along with load-balancing options for each. • Secure access to an application hosted within Azure or on-premises from the internet using Azure Application Gateway • Load balancing of incoming connections from the internet to resources in Azure using Azure External Load Balancer • Load balance connections from VM's not on the internet. e.g. - from VM's or DB Services using Azure Internal Load Balancer • Global load balancing across different geographic regions with maximum availability using Azure Traffic Manager For more information, see: Azure Application Gateway Azure External (Public) Load Balancer Azure Internal (private) Load Balancer Azure Traffic Manager	Azure Application Gateway Azure External Load Balancer Azure Internal Load Balancer Azure Traffic Manager

Azure Security Best Practice	Disable RDP/SSH access to virtual machines
Background	
It is possible to reach Azure virtual machines by using Remote Desktop Protocol (RDP) and the Secure Shell (SSH) protocol. These protocols enable the management VMs from remote locations and are standard in datacenter computing. The potential security problem with using these protocols over the internet is that attackers can use brute force techniques to gain access to Azure virtual machines. After the attackers gain access, they can use your VM as a launch point for compromising other machines on your virtual network or even attack networked devices outside Azure.	
Microsoft Guidance	**Azure Service Enabling**
We recommend that you disable direct RDP and SSH access to your Azure virtual machines from the internet. After direct RDP and SSH access from the internet is disabled, you have other options that you can use to access these VMs for remote management. - For single users, Point-to-Site VPN - For Multiple users, Site-to-Site VPN or Azure ExpressRoute For more information, see: VPN Gateway Point-to-Site VPN Gateway Site-to-Site Azure ExpressRoute	Azure Point-to-Site VPN Azure Site-to-Site VPN Azure ExpressRoute

Azure Security Best Practice	Secure your critical Azure service resources to only your virtual networks
Background	
Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your virtual network to the Azure service always remains on the Microsoft Azure backbone network.	
Microsoft Guidance	**Azure Service Enabling**
Use virtual network service endpoints to extend your virtual network private address space, and the identity of your virtual network to the Azure services, over a direct connection. For more information, see: Virtual Network - Service Endpoints	Azure Virtual Network Service Endpoints

4.4.3 Lock down and secure VM and computer operating systems

Azure Security Best Practice	Protect VMs by using authentication and access control

Background

The first step in protecting your VMs is to ensure that only authorized users can set up new VMs and access VMs.

Note: To improve the security of Linux VMs on Azure, you can integrate with Azure AD authentication. When you use Azure AD authentication for Linux VMs, you centrally control and enforce policies that allow or deny access to the VMs.

Microsoft Guidance	Azure Service Enabling
We recommend adhere to the guidance below in order to secure virtual machines: • Control VM Access by leveraging Azure Management Groups, Azure Policies and Azure Resource Groups • Secure privileged access using a least privileged approach leveraging built in Azure roles. For more information, see: Azure Policy Azure Resource Group Azure ARM - Management Groups Azure ARM - Resource Group Authoring Templates Implementing Least Privilege Administrative Models RBAC - Virtual Machine Contributor RBAC - Virtual Machine Contributor (classic) RBAC - Security Manager RBAC - DevTest Labs User Linux AD Authentication: Login to Linux Azure VM using Azure AD	Azure Management Groups Azure Policies Azure Resource Groups Azure Resource Manager Azure Roles
Reduce variability in your setup and deployment of VMs by using Azure Resource Manager For more information, see: Azure ARM - Management Azure Policy Azure Resource Groups Azure Roles	Azure Management Groups Azure Policy Azure Resource Groups Azure Resource Manager Azure Roles
Secure Privileged Access Use a least privilege approach and built-in Azure roles to enable users to access and set up VMs. Organizations that control VM access and setup improve their overall VM security. For more information regarding Azure roles, see: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles Note: Your subscription admins and co-admins can change this setting, making them administrators of all the VMs in a subscription. Be sure that you trust all your subscription admins and co-admins to log in to any of your machines. For more information, see: Azure ARM - Management Azure Policy Azure Resource Groups Azure Roles	Azure Management Groups Azure Policy Azure Resource Groups Azure Resource Manager Azure Roles

Azure Security Best Practice	Use multiple VMs for better availability
Background	
If your VM runs critical applications that need to have high availability, we strongly recommend that you use multiple VMs. For better availability, use an availability set. An availability set is a logical grouping that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they are deployed in an Azure datacenter. Azure ensures that the VMs you place in an availability set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or Azure software failure occurs, only a subset of your VMs are affected, and your overall application continues to be available to your customers. Availability sets are an essential capability when you want to build reliable cloud solutions.	
Microsoft Guidance	**Azure Service Enabling**
We recommend you use multiple VM's for better availability in conjunction with an Availability Set. For more information see: Azure VM Availability Set	Azure availability sets

Azure Security Best Practice	Protect against malware
Background	
You should install antimalware protection to help identify and remove viruses, spyware, and other malicious software. You can integrate Microsoft Antimalware and partner solutions with Azure Defender for Cloud for ease of deployment and built-in detections (alerts and incidents).	
Microsoft Guidance	**Azure Service Enabling**
Install anti-malware protection onto IaaS virtual machines & integrate with Microsoft Defender for Cloud You can install Microsoft Antimalware or a Microsoft partner's endpoint protection solution (Trend Micro, Symantec, McAfee, Windows Defender, and System Center Endpoint Protection). For more information see: Microsoft Defender for Cloud	Microsoft Defender

Azure Security Best Practice	Manage your VM Updates
Background	
Azure VMs, like all on-premises VMs, are meant to be user managed. Azure doesn't push Windows updates to them. You need to manage your VM updates.	
Microsoft Guidance	**Azure Service Enabling**
Ensure at deployment that images you built include the most recent round of Windows updates. Check for and install all Windows updates as a first step of every deployment. This measure is especially important to apply when you deploy images that come from either you or your own library. Although images from the Azure Marketplace are updated automatically by default, there can be a lag time (up to a few weeks) after a public release. It is recommended to periodically redeploy your VMs to force a fresh version of the OS. For more information, see: Azure Marketplace	Azure Marketplace
Install the latest security updates Some of the first workloads that customers move to Azure are labs and external-facing systems. If your Azure VMs host applications or services that need to be accessible to the internet, be vigilant about patching. Patch beyond the operating system. Unpatched vulnerabilities on partner applications can also lead to problems that can be avoided if good patch management is in place. For more information, see: Azure VM Guest Patching	Azure Automatic VM Patching
Deploy and test a backup solution. A backup needs to be handled the same way that you handle any other operation. This is true of systems that are part of your production environment extending to the cloud. Azure Backup can be used to help address your backup requirements. For more information, see: Azure Backup	Azure Backup

Azure Security Best Practice	Manage your VM security posture
Background	
Cyberthreats are evolving. Safeguarding your VMs requires a monitoring capability that can quickly detect threats, prevent unauthorized access to your resources, trigger alerts, and reduce false positives.	
Microsoft Guidance	**Azure Service Enabling**
To monitor the security posture of your Windows and Linux VMs, use Defender for Cloud. In Defender for Cloud, safeguard your VMs by taking advantage of the following capabilities: - Apply OS security settings with recommended configuration rules. - Identify and download system security and critical updates that might be missing. - Deploy recommendations for endpoint antimalware protection. - Validate disk encryption. - Assess and remediate vulnerabilities. - Detect threats. Defender for Cloud can actively monitor for threats, and potential threats are exposed in security alerts. Correlated threats are aggregated in a single view called a security incident. For more information, see: Defender for Cloud	Defender For Cloud

Azure Security Best Practice	Monitor VM Performance
Background	
Resource abuse can be a problem when VM processes consume more resources than they should. Performance issues with a VM can lead to service disruption, which violates the security principle of availability. This is particularly important for VMs that are hosting IIS or other web servers because high CPU or memory usage might indicate a denial of service (DoS) attack. It's imperative to monitor VM access not only reactively while an issue is occurring, but also proactively against baseline performance as measured during normal operation.	
Microsoft Guidance	**Azure Service Enabling**
We recommend that you use Azure Monitor to gain visibility into your resource's health. Azure Monitor features: - Resource diagnostic log files: Monitors your VM resources and identifies potential issues that might compromise performance and availability. - Azure Diagnostics extension: Provides monitoring and diagnostics capabilities on Windows VMs. You can enable these capabilities by including the extension as part of the Azure Resource Manager template. For more information, see: Azure Monitor	Azure Monitor

Azure Security Best Practice	Encrypt your virtual hard disk files

Background

Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.

Microsoft Guidance	Azure Service Enabling
Enable encryption on VMs. Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication. Create an Azure AD application for this purpose. For authentication purposes, you can use either client secret-based authentication or client certificate-based Azure AD authentication. For more information, see: Azure Disk Encryption VMS VMSS Azure AD Certificate based authentication	Azure Disk Encryption
Use a key encryption key (KEK) for an additional layer of security for encryption keys. Add a KEK to your key vault. Use the Add-AzKeyVaultKey cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises hardware security module (HSM) for key management. When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to Key Vault. Keeping an escrow copy of this key in an on-premises key management HSM offers additional protection against accidental deletion of keys. For more information, see: Azure Key Vault Azure Key Vault - HSM Protected Keys	Azure Key Vault
Take a snapshot and/or backup before disks are encrypted. Backups provide a recovery option if an unexpected failure happens during encryption. VMs with managed disks require a backup before encryption occurs. After a backup is made, you can use the Set-AzVMDiskEncryptionExtension cmdlet to encrypt managed disks by specifying the -skipVmBackup parameter. For more information, see: Backup Azure VMS Encryption	Azure Backup
Create and use a key vault that is in the same region as the VM to be encrypted. To make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the key vault and the VMs to be located in the same region. When you apply Azure Disk Encryption, you can satisfy the following business needs: • IaaS VMs are secured at rest through industry-standard encryption technology to address organizational security and compliance requirements. • IaaS VMs start under customer-controlled keys and policies, and you can audit their usage in your key vault. For more information, see: Azure Key Vault	Azure Key Vault

Azure Security Best Practice	Restrict Direct Internet Connectivity
Background	
Attackers constantly scan public cloud IP ranges for open management ports and attempt “easy” attacks like common passwords and known unpatched vulnerabilities.	
Microsoft Guidance	**Azure Service Enabling**
Prevent inadvertent exposure to network routing and security. Use Azure RBAC to ensure that only the central networking group has permission to networking resources.	Azure RBAC
Identify and remediate exposed VMs that allow access from “any” source IP address. Use Defender for Cloud. Defender for Cloud will recommend that you restrict access through internet-facing endpoints if any of your network security groups has one or more inbound rules that allow access from “any” source IP address. Security Center will recommend that you edit these inbound rules to restrict access to source IP addresses that actually need access. For more information, see: Protect network resources	Defender for Cloud
Restrict management ports (RDP, SSH) Just-in-time (JIT) VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. When JIT is enabled, Security Center locks down inbound traffic to your Azure VMs by creating a network security group rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the JIT solution. For more information, see: Secure your management ports with just-in-time access	Azure Privileged Access Management

4.4.4 Protect Data

Azure Security Best Practice	Manage with secure workstations
Background	
Because the vast majority of attacks target the end user, the endpoint becomes one of the primary points of attack. An attacker who compromises the endpoint can use the user’s credentials to gain access to the organization’s data. Most endpoint attacks take advantage of the fact that users are administrators in their local workstations. These secure management workstations can help you mitigate some of these attacks and ensure that your data is safer.	
Microsoft Guidance	**Azure Service Enabling**
Use a privileged access workstation to reduce the attack surface in workstations For more information, see: Securing devices as part of the privileged access story	N/A
Enforce security policies across all devices that are used to consume data, regardless of the data location (cloud or on-premises)	N/A

Azure Security Best Practice	Protect data at rest
Background	
Data encryption at rest is a recommended step toward data privacy, compliance, and data sovereignty.	
Microsoft Guidance	**Azure Service Enabling**
We recommend that you deploy Azure Disk Encryption. Azure Disk Encryption enables IT administrators to encrypt Windows and Linux IaaS VM disks. Disk Encryption combines the industry-standard Windows BitLocker feature and the Linux dm-crypt feature to provide volume encryption for the OS and the data disks. Azure Storage and Azure SQL Database encrypt data at rest by default, and many services offer encryption as an option. You can use Azure Key Vault to maintain control of keys that access and encrypt your data. For more information, see: Azure Security Disk Encryption Azure resource providers encryption model support	Azure Disk Encryption

Azure Security Best Practice	Protect data in transit
Background	
Protecting data in transit should be an essential part of your data protection strategy. Because data is moving back and forth from many locations, we generally recommend that you always use SSL/TLS protocols to exchange data across different locations. In some circumstances, you might want to isolate the entire communication channel between your on-premises and cloud infrastructures by using a VPN. For data moving between your on-premises infrastructure and Azure, consider appropriate safeguards such as HTTPS or VPN. When sending encrypted traffic between an Azure virtual network and an on-premises location over the public internet, use Azure VPN Gateway.	
Microsoft Guidance	**Azure Service Enabling**
Secure access from multiple workstations located on-premises to an Azure virtual network by using a site-to-site VPN. For more information, see: Create a Site-to-Site connection in the Azure portal	Azure VPN Gateway
Secure access from an individual workstation located on-premises to an Azure virtual network by using a point-to-site VPN. For more information, see: Configure a Point-to-Site connection by using certificate authentication (classic)	Azure VPN Gateway

Azure Security Best Practice	Secure email, documents, and sensitive data

Background

You want to control and secure email, documents, and sensitive data that you share outside your company. Azure Information Protection is a cloud-based solution that helps an organization to classify, label, and protect its documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users get recommendations.

Classification is identifiable at all times, regardless of where the data is stored or with whom it's shared. The labels include visual markings such as a header, footer, or watermark. Metadata is added to files and email headers in clear text. The clear text ensures that other services, such as solutions to prevent data loss, can identify the classification and take appropriate action.

The protection technology uses Azure Rights Management (Azure RMS). This technology is integrated with other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory. This protection technology uses encryption, identity, and authorization policies. Protection that is applied through Azure RMS stays with the documents and emails, independently of the location—inside or outside your organization, networks, file servers, and applications.

Organizations that are weak on data classification and file protection might be more susceptible to data leakage or data misuse. With proper file protection, you can analyze data flows to gain insight into your business, detect risky behaviors and take corrective measures, track access to documents, and so on.

Microsoft Guidance	Azure Service Enabling
Deploy Azure Information Protection. As part of the deployment, classify data assets into categories that reflect your content owner requirements. In addition, Configure usage logging for Azure RMS. Organizations that are weak on data classification and file protection might be more susceptible to data leakage or data misuse. With proper file protection, you can analyze data flows to gain insight into your business, detect risky behaviors and take corrective measures, track access to documents, and so on. For more information, see: Azure Information Protection deployment roadmap Logging and analyzing the protection usage from Azure Information Protection Data Classification for Cloud Readiness	Azure Information Protection Usage Logging for Azure RMS

4.4.5 Secure Databases

Azure Security Best Practice	Protect your data by using encryption
Background	
Azure SQL Database transparent data encryption helps protect data on disk and protects against unauthorized access to hardware. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. Transparent data encryption encrypts the storage of an entire database by using a symmetric key called the database encryption key. Even when the entire storage is encrypted, it is important to also encrypt the database itself. This is an implementation of the defense-in-depth approach for data protection. If you are using Azure SQL Database and want to protect sensitive data (such as credit card or social security numbers), you can encrypt databases with FIPS 140-2 validated 256-bit AES encryption. This encryption meets the requirements of many industry standards (for example, HIPAA and PCI).	
Microsoft Guidance	**Azure Service Enabling**
Enable SQL Server Transparent Data Encryption Files related to buffer pool extension (BPE) are not encrypted when you encrypt a database by using transparent data encryption. You must use file-system-level encryption tools like BitLocker or the Encrypting File System (EFS) for BPE-related files. Because an authorized user like a security administrator or a database administrator can access the data even if the database is encrypted with transparent data encryption, you should also follow these recommendations: - Enable SQL Server authentication at the database level. - Use Azure AD authentication by using RBAC roles. - Make sure that users and applications use separate accounts to authenticate. This way, you can limit the permissions granted to users and applications and reduce the risk of malicious activity. - Implement database-level security by using fixed database roles (such as db_datareader or db_datawriter). Or you can create custom roles for your application to grant explicit permissions to selected database objects. For other ways to encrypt your data, consider: - Cell-level encryption to encrypt specific columns or even cells of data with different encryption keys. - Always Encrypted, which allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine (SQL Database or SQL Server). As a result, Always Encrypted provides a separation between those who own the data (and can view it) and those who manage the data (but should have no access). - Row-Level Security, which enables customers to control access to rows in a database table based on the characteristics of the user who is executing a query. (Example characteristics are group membership and execution context.) Organizations that are not using database-level encryption might be more susceptible to attacks that compromise data located in SQL databases. For more information, see: Transparent data encryption for SQL Database, SQL Managed Instance, and Azure Synapse Analytics	Azure SQL TDE

Azure Security Best Practice	Enable Database Auditing
Background	
Auditing can help you maintain regulatory compliance, understand database activity, and find discrepancies and anomalies that might point to business concerns or security violations. Auditing facilitates adherence to compliance standards but does not guarantee compliance. Auditing an instance of the SQL Server Database Engine or an individual database involves tracking and logging events. For SQL Server, you can create audits that contain specifications for server-level events and specifications for database-level events. Audited events can be written to the event logs or to audit files.	
Microsoft Guidance	**Azure Service Enabling**
Enable SQL Database Auditing For more information, see: SQL Database Auditing	Azure SQL Database

Azure Security Best Practice	Enable Database Threat Protection
Background	
Threat protection goes beyond detection. Database threat protection includes: - Discovering and classifying your most sensitive data so you can protect your data. - Implementing secure configurations on your database so you can protect your database. - Detecting and responding to potential threats as they occur so you can quickly respond and remediate.	
Microsoft Guidance	**Azure Service Enabling**
Discover, classify, and label the sensitive data in your databases. Classify the data in your SQL database by enabling Data Discovery and Classification in Azure SQL Database. You can monitor access to your sensitive data in the Azure dashboard or download reports. For more information, see: SQL Data Discovery & Classification	Azure SQL Database
Track database vulnerabilities so you can proactively improve your database security. Use the Azure SQL Database Vulnerability Assessment service, which scans for potential database vulnerabilities. The service employs a knowledge base of rules that flag security vulnerabilities and show deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data. The rules are based on Microsoft best practices and focus on the security issues that present the biggest risks to your database and its valuable data. They cover both database-level issues and server-level security issues, like server firewall settings and server- level permissions. These rules also represent many of the requirements from regulatory bodies to meet their compliance standards. For more information, see: SQL Vulnerability Assessment	Azure Defender for SQL

Deploy Azure Defender for SQL ATP for Azure is unified package for advanced SQL security capabilities. It includes the services mentioned earlier: Data Discovery and Classification, Vulnerability Assessment, and Threat Detection. It provides a single location for enabling and managing these capabilities. Enabling these capabilities helps you: - Meet data privacy standards and regulatory compliance requirements. - Control access to your databases and harden their security. - Monitor a dynamic database environment where changes are hard to track. - Detect and respond to potential threats. In addition, Threat Detection integrates alerts with Azure Defender for Cloud for a central view of the security state of all of your Azure resources. For more information, see: Azure Defender for SQL	Azure Defender for SQL

4.4.6 Define and deploy strong operational security practices

Azure Security Best Practice	**Manage & Monitor User Passwords**
Background	
Effectively manage passwords, monitor and detect suspicious behavior.	
Microsoft Guidance	**Azure Service Enabling**
Ensure you have the proper level of password protection in the cloud. Follow the guidance in Microsoft Password Guidance, which is scoped to users of the Microsoft identity platforms (Azure Active Directory, Active Directory, and Microsoft account). For more information, see: Password Guidance	Azure AD
Monitor for suspicious actions related to your user accounts using Azure Directory Reports. Monitor for users at risk and risky sign-ins by using Azure Directory Reports. For more information, see: AD User at Risk Monitoring AD Risk Events Monitoring AD Monitoring - Security Reports	Active Directory Reports
Automatically detect and remediate high-risk passwords. Azure AD Identity Protection is a feature of the Azure AD Premium P2 edition that enables you to: - Detect potential vulnerabilities that affect your organization's identities - Configure automated responses to detected suspicious actions that are related to your organization's identities - Investigate suspicious incidents and take appropriate actions to resolve them For more information, see: AD Identity Protection	Azure Identity Protection

Azure Security Best Practice	Receive incident notifications from Microsoft
Background	
Be sure your security operations team receives Azure incident notifications from Microsoft. An incident notification lets your security team know you have compromised Azure resources so they can quickly respond to and remediate potential security risks.	
Microsoft Guidance	**Azure Service Enabling**
Configure incident notifications in In the Azure enrolment portal You can ensure admin contact information includes details that notify security operations. Contact information is an email address and phone number. For more information, see: Azure Portal	Azure Portal

Azure Security Best Practice	Organize Azure subscriptions into management groups
Background	
If your organization has many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope that is above subscriptions. You organize subscriptions into containers called management groups and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group.	
Microsoft Guidance	**Azure Service Enabling**
Ensure that new subscriptions apply governance elements like policies and permissions as they are added. Use the root management group to assign enterprise- wide security elements that apply to all Azure assets. Policies and permissions are examples of elements. For more information, see: Azure ARM - Management	Azure Management Groups
Align the top levels of management groups with segmentation strategy to provide a point for control and policy consistency within each segment. Create a single management group for each segment under the root management group. Don't create any other management groups under the root. For more information, see: Azure ARM - Management	Azure Management Groups
Limit management group depth to avoid confusion that hampers both operations and security. Limit your hierarchy to three levels, including the root. For more information, see: Azure ARM - Management	Azure Management Groups
Carefully select which items to apply to the entire enterprise with the root management group. Ensure root management group elements have a clear need to be applied across every resource and that they are low impact. Good candidates include: - Regulatory requirements that have a clear business impact (for example, restrictions related to data sovereignty) - Requirements with near-zero potential negative affect on operations, like policy with audit effect or RBAC permission assignments that have been carefully reviewed For more information, see: Azure ARM - Management	Azure Management Groups

Carefully plan and test all enterprise- wide changes on the root management group before applying them (policy, RBAC model, and so on). Changes in the root management group can affect every resource on Azure. While they provide a powerful way to ensure consistency across the enterprise, errors or incorrect usage can negatively affect production operations. Test all changes to the root management group in a test lab or production pilot. For more information, see: Azure ARM - Management	Azure Management Groups

Azure Security Best Practice	**Streamline environment creation with blueprints**
Background	
The Azure Blueprints service enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand-up new environments with a set of built-in components and the confidence that they're creating those environments within organizational compliance.	
Microsoft Guidance	**Azure Service Enabling**
Leverage Azure Blueprints to simplify largescale Azure deployments. Leverage Azure Resource Manager templates and role-based access controls and policies in a single blueprint definition. For more information, see: Azure Blueprints	Azure Blueprints

Azure Security Best Practice	**Monitor storage services for unexpected changes in behavior**
Background	
Diagnosing and troubleshooting issues in a distributed application hosted in a cloud environment can be more complex than it is in traditional environments. Applications can be deployed in a PaaS or IaaS infrastructure, on-premises, on a mobile device, or in some combination of these environments. Your application's network traffic might traverse public and private networks, and your application might use multiple storage technologies.	
Microsoft Guidance	**Azure Service Enabling**
Continuously monitor the storage services that your application uses for any unexpected changes in behavior (such as slower response times). Use logging to collect more detailed data and to analyze a problem in depth. The diagnostics information that you obtain from both monitoring and logging helps you to determine the root cause of the issue that your application encountered. Then you can troubleshoot the issue and determine the appropriate steps to remediate it. Azure Storage Analytics performs logging and provides metrics data for an Azure storage account. We recommend that you use this data to trace requests, analyze usage trends, and diagnose issues with your storage account. For more information, see: Azure Storage Analytics	Azure Storage Analytics

Azure Security Best Practice	Prevent, detect, and respond to threats
Background	
Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms. Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyber-attacks, and streamline security management. Because it's natively integrated, deployment of Defender for Cloud is easy, providing you with simple auto provisioning to secure your resources by default.	
Microsoft Guidance	**Azure Service Enabling**
Leverage Microsoft Defender for Cloud to continuously monitor your Azure environment Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises: - Continuously Assess - Secure - Defend For more information, see: Defender for Cloud	Microsoft Defender for Cloud

Azure Security Best Practice	Prevent, detect, and respond to threats
Background	
Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.	
Microsoft Guidance	**Azure Service Enabling**
Leverage Azure Sentinel to detect malicious activity within your Azure cloud and on-premises environments Sentinel includes the following capabilities: • Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. • Detect previously undetected threats and minimize false positives using Microsoft's analytics and unparalleled threat intelligence. • Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft. • Respond to incidents rapidly with built-in orchestration and automation of common tasks. For more information, see: Microsoft Sentinel	Microsoft Sentinel

Azure Security Best Practice	Prevent, detect, and respond to threats
Background	
Find the most serious security vulnerabilities so you can prioritize investigation.	
Microsoft Guidance	**Azure Service Enabling**
Review your Azure secure score to see the recommendations resulting from the Azure policies and initiatives built into Azure Defender for Cloud. These recommendations help address top risks like security updates, endpoint protection, encryption, security configurations, missing WAF, internet connected VMs, and many more. The secure score, which is based on Center for Internet Security (CIS) controls, lets you benchmark your organization's Azure security against external sources. External validation helps validate and enrich your team's security strategy. For more information, see: Secure score in Microsoft Defender for Cloud	Azure Secure Score

Azure Security Best Practice	Prevent, detect, and respond to threats
Background	
Integrate alerts to ensure the appropriate action is taken	
Microsoft Guidance	**Azure Service Enabling**
Integrate Defender for Cloud alerts into your security information and event management (SIEM) solution. Most organizations with a SIEM use it as a central clearinghouse for security alerts that require an analyst response. Processed events produced by Defender for Cloud are published to the Azure Activity Log, one of the logs available through Azure Monitor. Azure Monitor offers a consolidated pipeline for routing any of your monitoring data into a SIEM tool. For more information, see: Secure score in Microsoft Defender for Cloud Connect security alerts from Microsoft Defender for Cloud	Microsoft Defender for Cloud

Azure Security Best Practice	Prevent, detect, and respond to threats
Background	
Integrate Azure logs with your SIEM	
Microsoft Guidance	**Azure Service Enabling**
Use Azure Monitor to gather and export data This practice is critical for enabling security incident investigation, and online log retention is limited. If you are using Azure Sentinel, see the link below: Microsoft Sentinel data connectors	Azure Monitor Microsoft Sentinel

Azure Security Best Practice	Prevent, detect, and respond to threats
Background	
Speed up your investigation and hunting processes and reduce false positives by integrating Endpoint Detection and Response (EDR) capabilities into your attack investigation.	
Microsoft Guidance	**Azure Service Enabling**
Enable Windows Defender ATP integration via your Security Center security policy. Consider using Azure Sentinel for threat hunting and incident response. For more information, see: Microsoft Defender for Endpoint	Microsoft Defender for Endpoint

Azure Security Best Practice	Monitor end-to-end scenario-based network monitoring
Background	
Customers build an end-to-end network in Azure by combining network resources like a virtual network, ExpressRoute, Application Gateway, and load balancers. Monitoring is available on each of the network resources. Azure Network Watcher is a regional service. Use its diagnostic and visualization tools to monitor and diagnose conditions at a network scenario level in, to, and from Azure.	
Microsoft Guidance	**Azure Service Enabling**
Automate remote network monitoring with packet capture. Monitor and diagnose networking issues without logging in to your VMs by using Network Watcher. Trigger packet capture by setting alerts and gain access to real-time performance information at the packet level. When you see an issue, you can investigate in detail for better diagnoses. For more information, see: Azure Network Watcher	Azure Network Watcher
Gain insight into your network traffic by using flow logs. Build a deeper understanding of your network traffic patterns by using network security group flow logs. Information in flow logs helps you gather data for compliance, auditing, and monitoring your network security profile. For more information, see: Azure Network Watcher NSG Flow Logging	Azure Flow Logs
Diagnose VPN connectivity issues. Use Network Watcher to diagnose your most common VPN Gateway and connection issues. You can not only identify the issue but also use detailed logs to further investigate. For more information, see: Network Watcher - Diagnose on-premises connectivity	Azure Network Watcher

Azure Security Best Practice	Secure deployment by using proven DevOps tools
Background	
Use DevOps best practices to ensure that your enterprise and teams are productive and efficient	
Microsoft Guidance	**Azure Service Enabling**
Automate the build and deployment of services. Infrastructure as code is a set of techniques and practices that help IT pros remove the burden of day-to-day build and management of modular infrastructure. It enables IT pros to build and maintain their modern server environment in a way that is like how software developers build and maintain application code. You can use Azure Resource Manager to provision your applications by using a declarative template. In a single template, you can deploy multiple services along with their dependencies. You use the same template to repeatedly deploy your application in every stage of the application lifecycle. For more information, see: Azure ARM - Resource Group Authoring Templates	Azure Resource Manager
Automatically build and deploy to Azure web apps or cloud services. You can configure your Azure DevOps projects to automatically build and deploy to Azure web apps or cloud services. Azure DevOps automatically deploys the binaries after doing a build to Azure after every code check-in. The package build process is equivalent to the Package command in Visual Studio, and the publishing steps are equivalent to the Publish command in Visual Studio. For more information, see: Azure DevOps	Azure Pipelines
Automate release management. Azure Pipelines is a solution for automating multiple- stage deployment and managing the release process. Create managed continuous deployment pipelines to release quickly, easily, and often. With Azure Pipelines, you can automate your release process, and you can have predefined approval workflows. Deploy on-premises and to the cloud, extend, and customize as required. For more information, see: Azure Pipelines	Azure Pipelines
Check your app's performance before you launch it or deploy updates to production. Run cloud-based load tests to: • Find performance problems in your app. • Improve deployment quality. • Make sure that your app is always available. • Make sure that your app can handle traffic for • your next launch or marketing campaign. • Apache JMeter is a free, popular open-source tool with a strong community backing.	N/A
Monitor Application Performance Azure Application Insights is an extensible application performance management (APM) service for web developers on multiple platforms. Use Application Insights to monitor your live web application. It automatically detects performance anomalies. It includes analytics tools to help you diagnose issues and to understand what users actually do with your app. It is designed to help you continuously improve performance and usability. For more information, see: Azure Application Insights	Azure Application Insights

Azure Security Best Practice	Mitigate and protect against DDoS
Background	
Distributed denial of service (DDoS) is a type of attack that tries to exhaust application resources. The goal is to affect the application's availability and its ability to handle legitimate requests. These attacks are becoming more sophisticated and larger in size and impact. They can be targeted at any endpoint that is publicly reachable through the internet. Designing and building for DDoS resiliency requires planning and designing for a variety of failure modes.	
Microsoft Guidance	**Azure Service Enabling**
Ensure that security is a priority throughout the entire lifecycle of an application, from design and implementation to deployment and operations. Applications can have bugs that allow a relatively low volume of requests to use a lot of resources, resulting in a service outage. To help protect a service running on Microsoft Azure, you should have a good understanding of your application architecture and focus on the five pillars of software quality. You should know typical traffic volumes, the connectivity model between the application and other applications, and the service endpoints that are exposed to the public internet. Ensuring that an application is resilient enough to handle a denial of service that's targeted at the application itself is most important. Security and privacy are built into the Azure platform, beginning with the Security Development Lifecycle. The SDL addresses security at every development phase and ensures that Azure is continually updated to make it even more secure. For more information, see: Microsoft Azure Well-Architected Framework Microsoft Security Development Lifecycle	Azure Secure Development Lifecycle

Azure Security Best Practice	Mitigate and protect against DDoS
Background	
If your application depends on a single instance of a service, it creates a single point of failure. Provisioning multiple instances makes your system more resilient and more scalable.	
Microsoft Guidance	**Azure Service Enabling**
Design your applications to scale horizontally to meet the demand of an amplified load, specifically in the event of a DDoS attack. For Azure App Service, select an App Service plan that offers multiple instances. For Azure Cloud Services, configure each of your roles to use multiple instances. For Azure Virtual Machines, ensure that your VM architecture includes more than one VM and that each VM is included in an availability set. We recommend using virtual machine scale sets for autoscaling capabilities. For more information, see: Azure App Service Azure App Service plan Overview of Azure Cloud Services (classic) Azure Virtual Machine Scale Sets	Azure App Service Azure Virtual Machines Azure Virtual Machine Scale Sets

Azure Security Best Practice	Mitigate and protect against DDoS
Background	
Layering security defenses in an application reduces the chance of a successful attack.	
Microsoft Guidance	**Azure Service Enabling**
Implement secure designs for your applications by using the built-in capabilities of the Azure platform The risk of attack increases with the size (surface area) of the application. Reduce the surface area by using whitelisting to close down the exposed IP address space and listening ports that are not needed on the load balancers (Azure Load Balancer and Azure Application Gateway). Network security groups are another way to reduce the attack surface. You can use service tags and application security groups to minimize complexity for creating security rules and configuring network security, as a natural extension of an application's structure. You should deploy Azure services in a virtual network whenever possible. This practice allows service resources to communicate through private IP addresses. Azure service traffic from a virtual network uses public IP addresses as source IP addresses by default. Using service endpoints switches service traffic to use virtual network private addresses as the source IP addresses when they are accessing the Azure service from a virtual network. We often see customers' on-premises resources getting attacked along with their resources in Azure. If you are connecting an on-premises environment to Azure, minimize exposure of on-premises resources to the public internet. For more information, see: Azure Load Balancer Azure Application Gateway Azure Virtual Network Security Virtual Network Security - Service Tags Virtual Network Security - Application Security Groups Virtual Network - Service Endpoints	Azure Load Balancer Azure Application Gateway Network Security Groups Azure Service Tags Application Security Groups Azure Service Endpoints

Azure Security Best Practice	Mitigate and protect against DDoS
Background	
Implement DDoS Protection to mitigate against attacks that target service availability	
Microsoft Guidance	**Azure Service Enabling**
Leverage Azure DDoS Protection Azure has two DDoS service offerings that provide protection from network attacks: • Basic protection is integrated into Azure by default at no additional cost. The scale and capacity of the globally deployed Azure network provides defense against common network- layer attacks through always-on traffic monitoring and real-time mitigation. Basic requires no user configuration or application changes and helps protect all Azure services, including PaaS services like Azure DNS. • Standard protection provides advanced DDoS mitigation capabilities against network attacks. It is automatically tuned to protect your specific Azure resources. Protection is simple to enable during the creation of virtual networks. It can also be done after creation and requires no application or resource changes. For more information, see: Azure DDoS Protection	Azure DDoS Protection

Azure Security Best Practice	Enable Azure Policy
Background	
Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies.	
Microsoft Guidance	**Azure Service Enabling**
Enable Azure Policy to monitor and enforce your organization's written policy. Follow the guidance below to facilitate this: • Start policy deployments in audit mode and then later progress to deny or remediate. Test and review the results of the audit effect before you move to deny or remediate. • Have the assigned role monitor compliance through the Azure portal or via the command line. • Document mapping in your organization's documentation or in the Azure policy itself by adding a reference to the organizational policy in the Azure policy description or the Azure policy initiative description. For more information, see: Azure Policy - Rule Structure Create and manage policies to enforce compliance	Azure Policy

Azure Security Best Practice	Monitor Azure AD risk reports
Background	
The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. Discovering compromised identities is no easy task. Azure AD uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user accounts. Each detected suspicious action is stored in a record called a risk event.	
Microsoft Guidance	**Azure Service Enabling**
Monitor Azure AD Risk Reports Refer to the "Users at Risk" and the "Risky Sign-In" reports. For more information, see: Azure Operational Security best practices User at Risk Monitoring Report Risky Sign-ins Monitoring Report	Azure AD Risk Reports

4.4.7 Design, build, and manage secure cloud applications

Azure Security Best Practice	Adopt a policy of identity as the primary security perimeter
Background	
When you are designing and managing cloud applications, it's important to change your focus from a network-centric approach to an identity-centric approach to perimeter security. With PaaS deployments, you shift from needing to control everything yourself to sharing responsibility with Microsoft.	
Microsoft Guidance	**Azure Service Enabling**
Secure your keys and credentials to secure your PaaS deployment. Losing keys and credentials is a common problem. You can use a centralized solution where keys and secrets can be stored in hardware security modules. Azure provides you an HSM in the cloud with Azure Key Vault. For more information, see: https://docs.microsoft.com/azure/key-vault/key-vault-whatis	Azure Key Vault
Do not put credentials and other secrets in source code or GitHub. The only thing worse than losing your keys and credentials is having an unauthorized party gain access to them. Attackers can take advantage of bot technologies to find keys and secrets stored in code repositories such as GitHub. Do not put key and secrets in these public code repositories.	N/A
Protect your VM management interfaces on hybrid PaaS and IaaS services by using a management interface that enables you to remote manage these VMs directly. Remote management protocols such as SSH, RDP, and PowerShell remoting can be used. In general, we recommend that you do not enable direct remote access to VMs from the internet. If possible, use alternate approaches like using virtual private networks in an Azure virtual network. If alternative approaches are not available, ensure that you use complex passphrases and two-factor authentication (such as Azure Multi-Factor Authentication). For more information, see: Azure AD MFA	Azure MFA

Use strong authentication and authorization platforms. Use federated identities in Azure AD instead of custom user stores. When you use federated identities, you take advantage of a platform- based approach and you delegate the management of authorized identities to your partners. A federated identity approach is especially important when employees are terminated, and that information needs to be reflected through multiple identity and authorization systems. Use platform-supplied authentication and authorization mechanisms instead of custom code. The reason is that developing custom authentication code can be error prone. Most of your developers are not security experts and are unlikely to be aware of the subtleties and the latest developments in authentication and authorization. Commercial code (for example, from Microsoft) is often extensively security reviewed. Use two-factor authentication. Two-factor authentication is the current standard for authentication and authorization because it avoids the security weaknesses inherent in username and password types of authentication. Access to both the Azure management (portal/remote PowerShell) interfaces and customer-facing services should be designed and configured to use Azure Multi- Factor Authentication. Use standard authentication protocols, such as OAuth2 and Kerberos. These protocols have been extensively peer reviewed and are likely implemented as part of your platform libraries for authentication and authorization. For more information, see: Azure AD MFA	Azure MFA

Azure Security Best Practice	**Use threat modelling during application design**
Background	
The Microsoft Security Development Lifecycle specifies that teams should engage in a process called threat modelling during the design phase.	
Microsoft Guidance	**Azure Service Enabling**
Leverage the Microsoft SDL To help facilitate this process, Microsoft has created the SDL Threat Modelling Tool. Modelling the application design and enumerating STRIDE threats across all trust boundaries can catch design errors early on. Refer to the Microsoft SDL and the Azure Threat Modelling Tool to help with this. For more information, see: Microsoft Security Development Lifecycle Azure Threat Modelling Tool	Microsoft SDL Azure Threat Modelling Tool

Azure Security Best Practice	Develop on Azure App Service

Background

Azure App Service is a PaaS offering that lets you create web and mobile apps for any platform or device and connect to data anywhere, in the cloud or on-premises. App Service includes the web and mobile capabilities that were previously delivered separately as Azure Websites and Azure Mobile Services. It also includes new capabilities for automating business processes and hosting cloud APIs. As a single integrated service, App Service brings a rich set of capabilities to web, mobile, and integration scenarios.

Microsoft Guidance	Azure Service Enabling
Authenticate through Azure Active Directory. App Service provides an OAuth 2.0 service for your identity provider. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, and mobile phones. Azure AD uses OAuth 2.0 to enable you to authorize access to mobile and web applications. For more information, see: Azure AD	Azure AD
Restrict access based on the need to know and least privilege security principles. Restricting access is imperative for organizations that want to enforce security policies for data access. You can use RBAC to assign permissions to users, groups, and applications at a certain scope. For more information, see: Azure AD RBAC	Azure Active Directory RBAC
Protect your keys. Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. With Key Vault, you can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs. See Azure Key Vault to learn more. You can also use Key Vault to manage your TLS certificates with auto-renewal. For more information, see: Azure Key Vault	Azure Key Vault
Restrict incoming source IP addresses. App Service Environment has a virtual network integration feature that helps you restrict incoming source IP addresses through network security groups. Virtual networks enable you to place Azure resources in a non-internet, routable network that you control access to. To learn more, see Integrate your app with an Azure virtual network. For more information, see: Azure App Service Azure App Service - Web sites integrate with VNet	Azure App Service
Monitor the security state of your App Service environments. Use Microsoft Defender for Cloud to monitor your App Service environments. When Defender identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls. Note: Monitoring App Service is in preview and available only on the Standard tier of Defender for Cloud. For more information, see: Microsoft Defender for Cloud	Microsoft Defender for Cloud

Azure Security Best Practice	Install a web application firewall

Background

Web applications are increasingly targets of malicious attacks that exploit commonly known vulnerabilities. Common among these exploits are SQL injection attacks, cross site scripting attacks to name a few. Preventing such attacks in application code can be challenging and may require rigorous maintenance, patching and monitoring at many layers of the application topology. A centralized web application firewall helps make security management much simpler and gives better assurance to application administrators against threats or intrusions. A WAF solution can also react to a security threat faster by patching a known vulnerability at a central location versus securing each of individual web applications. Existing application gateways can be converted to a web application firewall enabled application gateway easily.

Microsoft Guidance	Azure Service Enabling
Deploy Azure Web Application Firewall. Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities. WAF is based on rules from the OWASP (Open Web Application Security Project) core rule sets 3.0 or 2.2.9. For more information, see: Azure WAF OWASP ModSecurity Core Rule Set	Azure Web Application Firewall

Azure Security Best Practice	Monitor the performance of your applications

Background

Monitoring is the act of collecting and analyzing data to determine the performance, health, and availability of your application. An effective monitoring strategy helps you understand the detailed operation of the components of your application. It helps you increase your uptime by notifying you of critical issues so that you can resolve them before they become problems. It also helps you detect anomalies that might be security related.

Microsoft Guidance	Azure Service Enabling
Leverage Azure Application Insights to monitor availability, performance and health of your applications. Use Azure Application Insights to monitor availability, performance, and usage of your application, whether it is hosted in the cloud or on-premises. By using Application Insights, you can quickly identify and diagnose errors in your application without waiting for a user to report them. With the information that you collect, you can make informed choices on your application's maintenance and improvements. Application Insights has extensive tools for interacting with the data that it collects. Application Insights stores its data in a common repository. It can take advantage of shared functionality such as alerts, dashboards, and deep analysis with the Log Analytics query language. For more information, see: Azure Monitor - Application Insights	Azure Application Insights

Azure Security Best Practice	Perform security penetration testing
Background	
Validating security defenses is as important as testing any other functionality. Make penetration testing a standard part of your build and deployment process. Schedule regular security tests and vulnerability scanning on deployed applications, and monitor for open ports, endpoints, and attacks. Fuzz testing is a method for finding program failures (code errors) by supplying malformed input data to program interfaces (entry points) that parse and consume this data. Microsoft Security Risk Detection is a cloud-based tool that you can use to look for bugs and other security vulnerabilities in your software before you deploy it to Azure. The tool is designed to catch vulnerabilities before you deploy software, so you don't have to patch a bug, deal with crashes, or respond to an attack after the software is released.	
Microsoft Guidance	**Azure Service Enabling**
Perform Pen testing as part of the build and deployment process	**N/A**

4.5 Azure CAF Top 11 Security Best Practices

A detailed guidance for Azure best practice security recommendations is provided via Security Best Practices for Azure Solutions and Azure Security Best Practices and Patterns. But additionally, Cloud Adoption Framework (CAF) provides with a Top 11 Security Best Practices that have been formulated by Microsoft based on lessons learned from their customers as well their own Azure environments.

Following are the Azure Top 11 Security Best Practices[23]:

1. **People: Educate People about the cloud security journey**
   It is important that your team is aware about your cloud strategy, roadmap, and the overall cloud environment's shared responsibility model. Microsoft has published following lessons learned by their customers on their cloud journey:
   - How security roles and responsibilities are evolving - here
   - Evolution of threat environments, roles, and digital strategies - here
   - Transformation of security strategies, tools, and threats - here
   - Learnings from Microsoft experience securing hyperscale cloud environment - here

2. **People: Educate people on cloud security technology**
   To make sound informed decisions, it is important that technical teams have access to training and good understanding of the technologies in use for the services you provide to your customers. Microsoft provides with a learning path specifically focused on Azure Security technologies which can be found here

3. **Process: Assign accountability for cloud security decisions**
   Designate who is responsible for each aspect of the security within your Azure environment. Typical areas wherein security decisions are required include – Network Security, Network Management, Server Endpoint Security, Incident Monitoring and Response, IAM Policy Management, and Identity Security and Standards.

[23] https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-top-10

4. **Update incident response process for cloud**
   Update processes, prepare your team and practice with simulated attacks so that there is enough confidence and know-how during incident investigation, remediation, and threat hunting

5. **Process: Establish security posture management**
   Ensure that you are actively monitoring and managing your security posture within your Azure environment by assigning clear ownership of responsibilities and automating and simplifying tasks. Responsibilities are further divided into – security posture management (using Azure Security Centre scores) and security remediation which should achieved by assigning accountability to teams managing the respective resources

6. **Technology: Require Passwordless or Multi-Factor Authentication (MFA)**
   Mandate user authentication where possible (especially admin users) is enforced via MFA. Required for MFA should be mandated in the organization's IAM policy. Instructions for enabling MFA on Azure can be found here, Passwordless (via Windows Hello) can be found here and Passwordless (via authenticator app) here

7. **Technology: Integrate native firewall and network security**
   Simplify systems and data protection against network attacks by integrating Azure Firewall, Azure Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) mitigations into your network security approach. These security services are important basic security controls that can be implemented to protect applications and services from malicious attacks, and as these are native Azure capabilities it further simplifies implementation and operations. Additionally, Azure Marketplace includes many other third-party firewall providers. Following are some useful documentations for Azure native services:
   - Azure Firewall - here
   - Azure WAF - here
   - Azure DDoS protection - here

8. **Technology: Integrate native threat detection**
   By leveraging native threat detection and response capabilities with your existing SOC and SIEM platforms, you can simplify your overall threat detection and response strategy. Azure Security Centre (ASC) integrates with Azure Defender to provide cloud workload protection (CWP). Further details on enabling threat detection in ASC can be found here

9. **Architecture: Standardize on a single directory and identity**
   Simplify and standardize on a single directory and identity using Azure AD. Ensure to have single identity for each user and application in Azure. Managing multiple accounts and directories possibly creates an incentive for poor security practices e.g., same password across accounts etc. which can be further exploited by attackers. Further details on standardizing Azure AD can be found here

10. **Architecture: Use identity-based access control (instead of keys)**
    Use Azure AD instead of key-based authentication wherever possible (e.g., Azure services, applications, APIs etc.). Key-based authentication involves management of keys securely and its on-going maintenance. Identity-based authentication can provide mature capabilities to tackle challenges like secret rotation, lifecycle

management, administrative delegation etc. with key-based authentication. Further details for managing application identities securely and automatically can be found here

11. **Architecture: Establish a single unified security strategy**
    Ensure all teams are aligned to a single strategy that both enables and secures enterprise systems and data. Build and implement a security strategy for cloud that includes the input and active participation of all teams. Further details to build the overall strategy can be found here and to build a security strategy can be found here

Additionally, you can refer to detailed security best practices for Azure services using following documentation:

- Security Best Practices for Azure Solutions here
- Azure Security Best Practices and Patterns here
- Azure Security baselines here
- Azure security Benchmark here

4.6 Convergent's Cloud Security Best Practices

Convergent is the leading provider of risk assessment and compliance services for the media & entertainment sector, providing assurance to vendors and content owners that systems and applications on site and in cloud workflows are correctly configured and operated securely. The cloud security assessment is based on a well-defined list of security controls put together using cloud service provider best practices, CIS benchmarks, MPA best practices and application hardening guidelines. These controls along with Azure recommendations in previous section can provide with a comprehensive list of security recommendations and controls checklist that can be used when deploying services in Azure cloud platform.

Following is the list of Convergent recommended cloud security best practices:

1. **Personnel: Train staff on cloud technologies**
   Cloud misconfigurations remain one of the biggest risks to the services running on cloud platforms, and user error when configuring these services can potentially lead to security incidents that could be catastrophic for an organization. Training requirements might differ based on roles and responsibilities within an organization

   Recommendations: You can find more information on Microsoft learning pathways for Azure here

2. **Governance: Processes should be implemented and documented in policies**
   All the important and relevant processes like change management, incident management, security monitoring & alerting, patch management, secure development, risk management, vulnerability management, hardening guidelines, joiner-mover-leaver process, key management, architectural diagrams, and content workflow diagrams should be all documented with process in place periodically review and update them as required

3. **Governance: Policies should be in place to prevent misconfigurations**
   It is important to have appropriate tooling and procedures in place in-line with the policies that prevent misconfigurations when deploying services in Azure

Recommendations: Azure Governance solution can be used leveraging features like Azure Management Groups, Azure Policy, Azure Blueprints, Azure Resource Graph, and Cost Management & Billing. Azure Security Centre can also be used to add continuous monitoring. Further details for Azure Governance features can be found here

4. **Data Protection: Ensure data is protected in transit and at rest**
   To protect your data and to maintain confidentiality and integrity, some form of encryption functionality should be used

   Recommendations: Azure can support encryption at rest (enabling encryption on VMs, containers, databases etc.) and in transit functionalities (via TLS). Azure services like Azure Key vault and Customer Lockbox for Azure are commonly used. Further details on Azure encryption features can be found here

5. **Key Management: Keys and secrets should be securely stored and regularly rotated**
   Ensure that appropriate procedures are in place to manage and maintain keys and secrets as per policy

   Recommendations: Azure Key Vault service can be used for key management purposes. Further details for key vault can be found here

6. **Network Security: Use network segmentation and protect network resources with firewalls and DDoS protection**
   Cloud networks should be segmented and secured (e.g., subnets, VPCs, firewalls and DDoS protection). In addition, outbound internet access for virtual servers and containers should be controlled to only required destinations and service ports

   Recommendations: Azure Virtual Network (VNet), Azure Network Security Groups (NSGs), Azure Firewall and Azure DDoS protection are some of the azure services that can be leveraged. Further details on Azure network security can be found here

7. **Network Security: Use Web Application Firewalls (WAF) to protect internet facing applications and services**
   WAF services should be implemented to protect external facing applications and services. WAF rules should be implemented in-line with OWASP Top10 recommendations

   Recommendations: Azure WAF service can be leveraged following the best practice implementation guidelines. Further details for Azure WAF can be found here

8. **Vulnerability Management: Automated scanning and continuous monitoring tools should be in place**
   Virtual workloads, internet facing services, database, source codes, and compiled images for container-based applications should all be periodically scanned for vulnerabilities. Additionally, there should be tooling in place to monitor security misconfigurations and alerting functionality

   Recommendations: Microsoft defender for endpoint and Azure Defender are services that can be leveraged for vulnerability management for the workloads. ASC can be used for continuous monitoring and alerting functionality. Further details for vulnerability management functions in Azure can be found here

9. **Patch Management: Ensure that proper patch management process is in place for application and OS on VMs as well as for container-based applications**
   Appropriate patch management processes in place will ensure that the workloads all have up-to-date patch and updates installed and are regularly checked for vulnerabilities

   Recommendations: Azure update management service can be used to install updates on Windows and Linux VMs. Further details on patch management can be found here

10. **Anti-Malware: Deploy centrally managed anti-malware solution for virtual machines**
    Appropriate endpoint protection should in place for virtual machines. Selected solution must have central management capabilities

    Recommendations: Microsoft Antimalware for cloud services and VMs is a free service that can be leveraged for an anti-malware solution. Further details on this solution can be found here

11. **Security Logging: Enable audit logging for all the key services in use in Azure**
    All the key services used in Azure should be monitored and log retentions should be set for 12 months

    Recommendations: Azure Activity logs, Azure resource logs, Azure AD reporting logs, VMs and Cloud services logs, Azure storage analytics, NSG flow logs (Azure Network Watcher), Application Insight, Azure Monitor and ASC are the different types of logs that can be available on Azure. Further details for logging can be found here

12. **Active Security Monitoring: Ensure tooling is in place to monitor and detect malicious activity**
    Tools should be in place to monitor and detect malicious activity. Tools should have ability to corelate events and trigger alerts based on set conditions

    Recommendations: Azure Sentinel and Azure ASC are the services that can be leveraged for security monitoring. Further details for security monitoring using sentinel can be found here

13. **Active Security Monitoring: Ensure tools in place have appropriate alerting functionality in place to notify personnel**
    Depending on the tools used, it is important to ensure that there is some form alerting rules in place which notifies key personnel. In some instance you can utilize automation or orchestration functionalities for remediation

    Recommendations: Azure Sentinel and Azure ASC are the services that can be leveraged for this control. Further details for security monitoring using sentinel can be found here

14. **IAM: Deploy a centralized identity provider**
    Use a centrally deployed identity provider for user and application identities and access authentication. Ensure to enable multi-factor authentication (MFA) where possible and secure access into your cloud environment

    Recommendations: Azure AD service can be leveraged for IAM deployment. Further details can be found here

15. **Secure Testing: Engage 3rd party to perform security testing**
    Ensure 3rd party engagement is in place for annual cloud security assessment and penetration testing

16. **Secure Testing: Perform regular testing of controls**
    Ensure regular testing of controls is completed including simulation of malicious activity. This can form part of cyber security incident response plan of your organization

17. **Secure Coding: Store code securely and scan code for vulnerabilities**
    It is important to ensure that any code is stored in a secure repository and that it is regularly scanned for vulnerabilities

    Recommendations: Azure Repos can be leveraged for this control. Further details can be found here

18. **Secure Pipeline: Avoid manual configuration where possible, CI/CD tools should be leveraged**
    Where possible configurations should be deployed using automated CI/CD tools

    Recommendations: Azure pipeline is a service that can be leveraged for this control. Further details can be found here

19. **Hardening: Ensure appropriate hardening guidelines are in place**
    Hardening guidelines for servers, cloud services, container-based workloads and applications used for ingest/egest of content should be in place

    Recommendations: CIS benchmarks provide recommendations for hardening azure environment along with CIS hardened images. Admin guides for the relevant 3rd party applications used should be referred for application hardening guidelines. Further details regarding CIS can be found here

20. **Database Security: Ensure database auditing and security monitoring is enabled**
    Database services in use should be secured including the data at rest on them. Appropriate security monitoring should be in place for database services

    Recommendations: Azure Key Vault service can be used to manage encryption keys used to protect data at rest and TLS for data in transit. Database security checklist can be found here.

4.7 Convergent's Remote Worker Best Practices

Following are some of the Convergent recommended best practices for remote workers:

- Remote workers should undergo pre-employment screening and/or background checks according to a risk assessment (where permitted and applicable by local law)

- Content should not be re-distributed to sub-contractors or third-party operational service providers

- Remote workers should undertake security awareness training upon hiring, before being granted access to content, at the start of a new project, upon changes in security protocols, and at least annually thereafter
- Content handling should be in a private dedicated workspace
- Encrypt content on hard drives and/or encrypt entire hard drives (where possible) using a minimum of AES-256 encryption by either; File-based encryption (i.e., encrypting the content itself) or Drive-based encryption (i.e., encrypting the hard drive)
- Portable media (e.g., USB HDD) must be stored in a secured location (e.g., locked cabinet, safe, or other secure storage location)
- Do not print, store, or distribute content in hard-copy format
- All external remote access / connections must be disabled (e.g., team viewer)
- Local firewalls should be implemented on workstations, laptops, or mobile devices to restrict unauthorized access
- All workstations, laptops or mobile devices should be configured with a screensaver
- Anti-virus software must be installed and in use on all devices
- All devices, including storage devices, must have full hard disk encryption.
- Update all operating systems, firmware, software versions, and security signatures
- Store content on dedicated storage. Do not use personal ‘cloud-based' storage services or shared storage devices
- Do not use ‘personal’ cloud-based applications, subscriptions, or licensed services without prior written consent from the content owner
- Use a strong password on all devices that accesses content
- Content should only be transferred over client approved file-based transfer platforms.

4.8 Shared Responsibility Model

As you decide on a public cloud platform for your services, it is critical to understand which part of the environment you have full responsibility for, and which elements are looked after by your cloud service provider. Depending on the type of services you chose to consume, the shared responsibility model might apply to you differently e.g., if you are using IaaS based services on Azure – the responsibility of the physical hosts, network and datacenter is with Microsoft whereas everything else is your responsibility as the consumer of the service. Figure 28 – Azure Shared Responsibility Model below gives a high-level overview of the model.

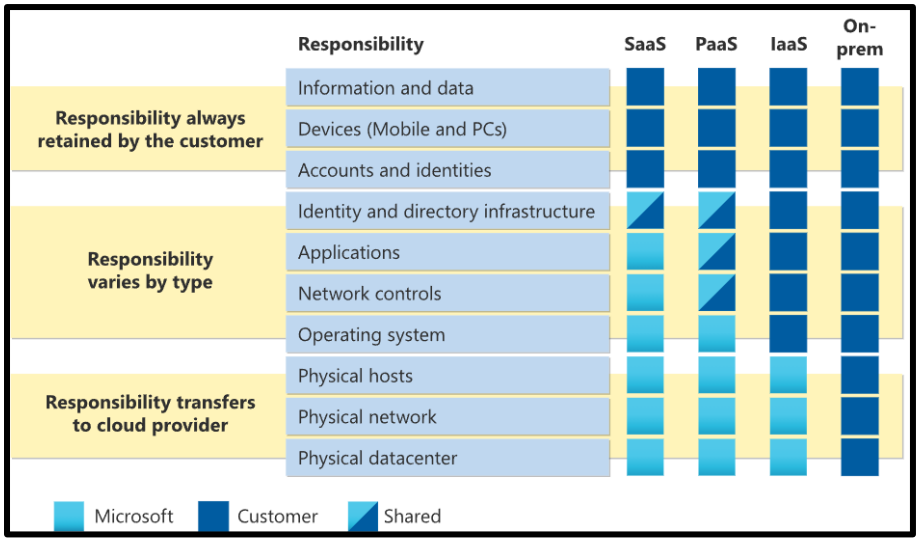

Figure 28 – Azure Shared Responsibility Model[24]

In any scenario, your data, and identities (along with on-premises resources) are your responsibility including their security and ensuring they are protected. Following are some of the responsibilities that always sits with the cloud consumer regardless of the type of services you are consuming:

- Data
- Endpoints
- Account
- Access Management

There are many advantages of leveraging a public cloud platform and one of them is how it helps with solving some of the information security challenges. Customers can leverage Azure's cloud native security capabilities to meet organization and compliance security controls and standards. Figure 29 – Cloud Security Advantages, gives a high-level overview on how cloud-enabled security is beneficial compared to traditional approach.

[24] https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

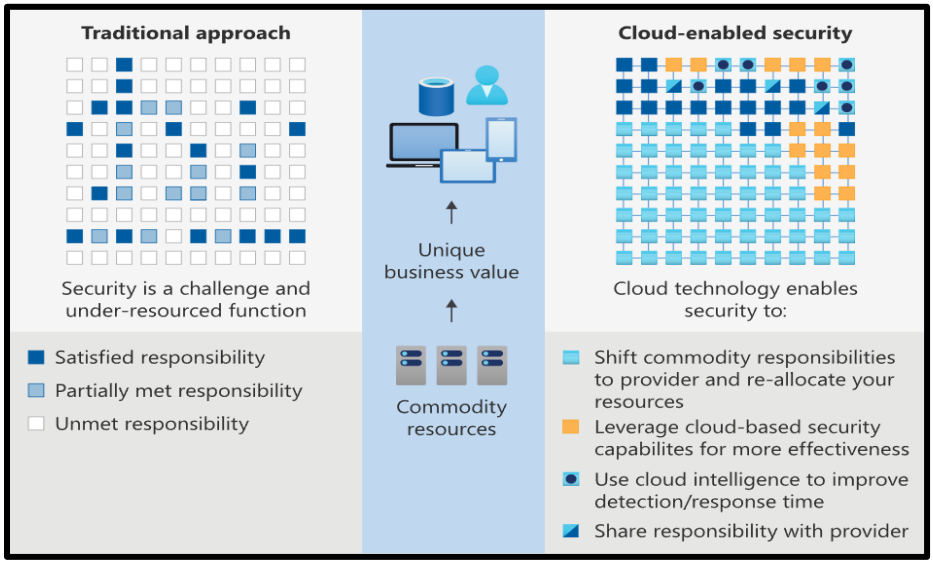

Figure 29 – Cloud Security Advantages[24]

[24] https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

5. Microsoft Cybersecurity Reference Architecture

Microsoft Cybersecurity Reference Architecture (MCRA) describes Microsoft's cybersecurity capabilities. These reference architectures cover a lot of different areas and describe how Microsoft security capabilities integrate with other Microsoft platforms e.g., Office365, Azure, etc. and 3rd party cloud platforms e.g., AWS, Google GCP etc. Figure 30 – Microsoft Security Capabilities gives a high-level overview on the key security capabilities on offer from Microsoft.

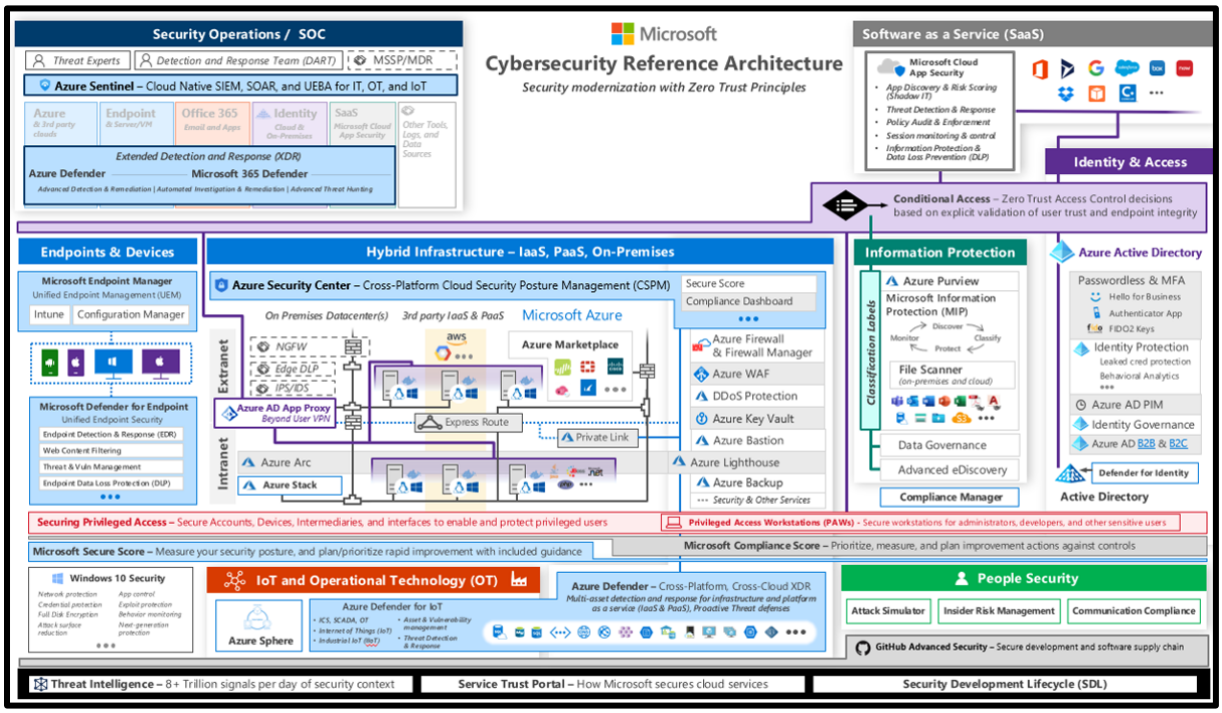

Figure 30 – Microsoft Cybersecurity Capabilities[25]

Anything that you decide to provision on a cloud platform should have an underlying security policy and strategy around it that ensures secure deployment of your services in cloud. Azure offers various native security control features that help you achieve this. It is also a common practice in large enterprises to have a multi-cloud deployment as part of their overall cloud strategy. Microsoft understands the importance of both these elements and hence has an MCRA in place for both Azure Native Security offerings and Multi-Cloud and Cross-Platform integration with Azure.

MCRAs are usually used for one of the following scenarios:

- A starting reference architecture for your environment's security architecture
- A comparison mechanism to understand what you currently have deployed and what does the reference architecture recommend
- Learn more about the respective Microsoft security capabilities on offer and how they can be applied to your environment
- Understand the different integration capabilities with third-party apps and cloud platforms and how you can align and integrate with your existing investment
- A tool used to learn and improve understanding on various cybersecurity concepts

[25] https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

The complete list of MCRAs and respective documentations can be found here.

5.1 MCRA – Azure Native Security

As discussed earlier in the document, there are a lot of different Azure native security offerings that can be leveraged when deploying your services securely in the cloud. Figure 31 – MCRA Native Security for Azure gives a high-level overview of the reference architecture that outlines key Azure cloud native security features that can be used as applicable to your organization's deployment.

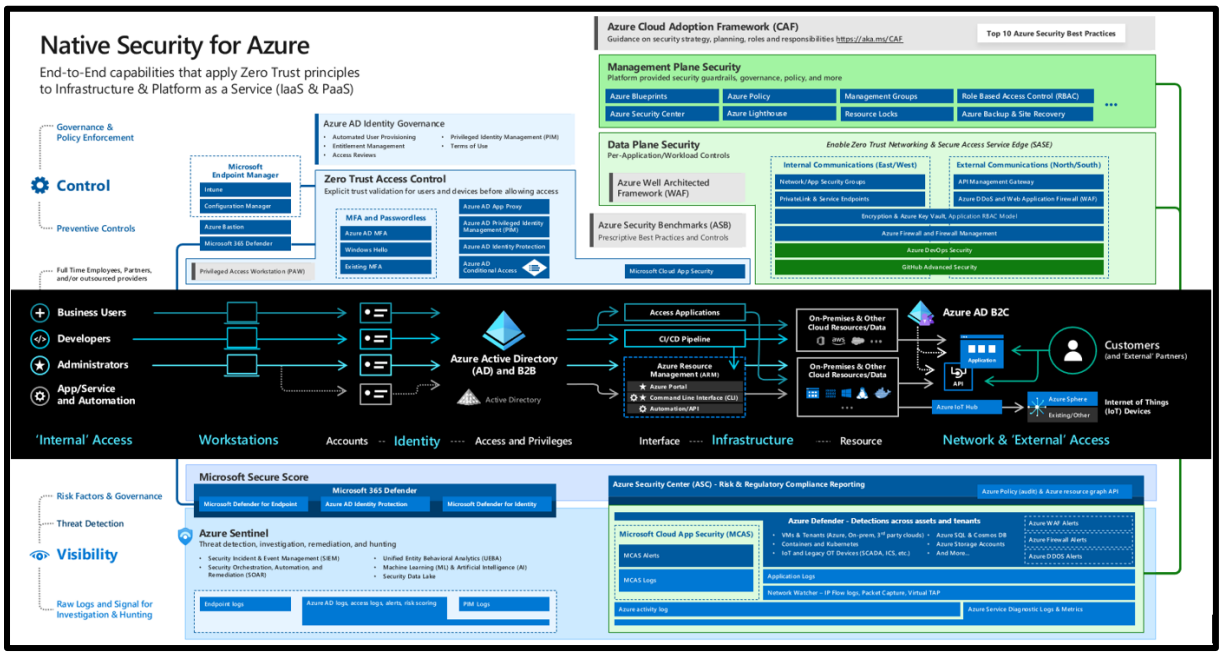

Figure 31 – MCRA Native Security for Azure[25]

MCRA Native Security for Azure breaks down different security services in several key areas that should be considered when deploying services in Azure, these include[25]:

- **Visibility & Control:** This will ensure that you can maintain Confidentiality, Integrity and Availability of the systems and data. Services like Azure Sentinel, Azure Security Centre (ASC), Azure Defender, Application Logs, Network Watcher, Azure Activity Logs, Azure Service Diagnostic Logs & Metrics and Microsoft Cloud Application Security (MCAS) Alerts and Logs can be used to achieve complete visibility and maintain proper control over your cloud environment
- **Protecting Access to Azure:** Using extended detection and response capabilities (XDR) e.g., Microsoft O365 Defender, logs for endpoint, identity etc. and zero trust access control practices that validates trust before granting access to Azure resources – can help to ensure that identities and devices connecting to Azure are secure

[25] https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

- **Management Plane Security:** Using software-defined data center capabilities security policies, roles and other controls are applied to the Azure workloads. This enables creation of guardrails for developers and workload users enforcing consistent security approach across your Azure environment. Azure Blueprints, Azure Policy, Management groups, RBAC, Azure Security Centre (ASC), Azure Lighthouse, Resource locks, and Azure Backup & Site Recovery are some of the native security offerings for management plane security

Additionally, it is worth considering Azure Cloud Adoption Framework (CAF) which provides guidance on cloud adoption strategy, performance, planning, governance, cost optimization, security etc. and Azure Security Baseline (ASB) which provides guidance on architecting workloads focusing on security, performance, cost optimization, reliability etc.

5.2 MCRA – Multi-Cloud & Cross-Platform

Multi-Cloud deployment is a standard cloud strategy that is commonly considered by large and medium enterprise customers. Whereas you might have a valid business case and justification for multi-cloud deployment, it is important to have a central monitoring and cross-platform integration between your choice of public cloud platforms.

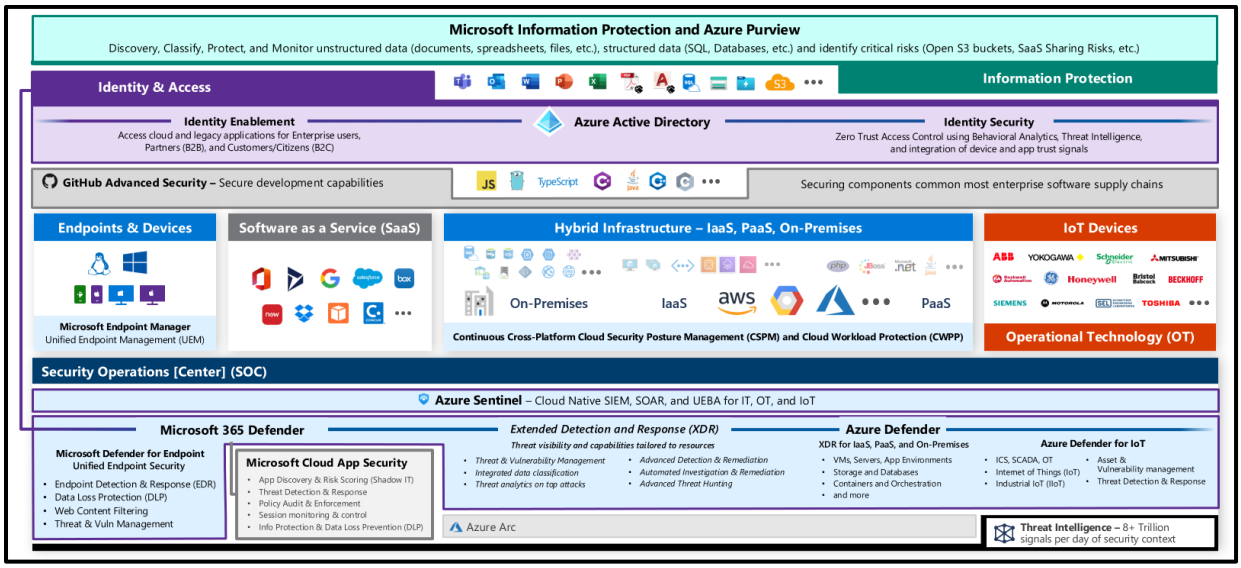

Figure 32 – MCRA Multi-Cloud & Cross-Platform[25]

Microsoft has built security for multi-cloud deployment by leveraging their partnership with global network of customers and partners spanning solution integration and MDR/MSSP partners, including organizations like NIST, CIS, The Open Group, CERTS, ISACs, Law Enforcement agencies (for botnet takedowns) etc. which can enable their customers to reduce risks in complex environments.

[25] https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

MCRA for Multi-Cloud & Cross-Platform breaks down key architecture components in the following sections[25]:

- **Endpoint and Cloud Management:** Microsoft endpoint manager provides a unified endpoint management (UEM) to manage endpoint devices across Mac, Android, iOS, and Windows OS. Cloud Security Posture Management (CSPM) provides insight into your multi-cloud and on-premises data center as well as Cloud Workload Protection capabilities (CWPP)
- **SIEM & XDR Strategy:** Azure sentinel (SIEM) platform ingests any logs from any source, correlates them and reasons over them with machine learning (ML) and user and entity behavioral analytics (UEBA), and automates response with Security Orchestration, Automation and Response (SOAR) which helps to provide a broad visibility across your environment. Extended Detection and Response (XDR) capabilities provide detection and response functionality which can be used to generate high quality alerts
- **Infrastructure XDR:** Azure Defender is the XDR for Azure services including VMs, App services, storage, SQL, Kubernetes, container registries etc. Using Azure Arc, you can extend Azure Defender to other public cloud platforms like AWS, GCP etc. and on-premises resources by projecting them into Azure objects, enabling management and security of those resources
- **Productivity and Identity XDR:** Microsoft O365 Defender provides an extensive library of pre-built SOAR capabilities as well as Web Content Filtering and integrated Threat and Vulnerability Management etc.
- **Identity Enablement and Security:** Azure AD provides comprehensive list of solutions for Identity Enablement for employees, partners (B2B) and customers (B2C) across any platform or cloud as well as Identity Security for use cases with Zero-Trust access control that explicitly verifies trust (via XDR) and users (via UEBA), Threat intelligence and analytics
- **Information Protection:** Microsoft Information Protection and Azure Purview provide a full lifecycle approach to discovering, classifying, protecting, and monitoring structured (SQL, databases etc.) and unstructured data (documents, spreadsheets, files etc.) as well as identifying critical risks (e.g., Open S3 buckets, SaaS sharing risks etc.)

[25] https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

6. Current and Future Technologies

There are various technologies which are worth considering improving your services' performance, availability, and overall user experience. Some of these include evolution to 5G networks for better network connection speeds, passwordless to improve your organization's overall IAM posture, and use of AI and ML to improve your processes and data analytics within your workflows. This section gives a high-level overview of these technologies and how Azure cloud platform can be leveraged for their implementation.

6.1 5G Networks

5G is the 5th generation wireless mobile network that can provide high speed network connections with low latency, better reliability improving overall availability for the end users. With technologies like IoT more devices are dependent on high-speed network connections than ever before. It is based on OFDM (Orthogonal frequency-division multiplexing) which modulates a digital signal across several different channels to reduce interference.

Azure Edge Zones and Azure Private Edge Zones deliver consistent Azure services, app platform and management to the edge with 5G providing support for additional use cases like development of distributed applications across cloud, on-premises and edge, local data processing for latency critical media services workloads, acceleration of IoT, AI and real-time analytics[26].

Figure 33 – Azure Private Edge Zones[26]

Azure private multi-access edge compute (MEC) is an evolution of Private Edge Zone. It is a solution that leverages multiple platforms and capabilities including edge services and applications, edge network functions, edge compute option and edge radios and devices.

Additional details for Azure Private MEC can be found here

[26] https://azure.microsoft.com/en-gb/blog/microsoft-partners-with-the-industry-to-unlock-new-5g-scenarios-with-azure-edge-zones/

6.2 Artificial Intelligence & Machine Learning

Machine Learning (ML) is the concept of machines being able to learn and adapt through experience and modelling processes (studying patterns in the data) whereas Artificial Intelligence (AI) makes use of ML, deep learning, and other capabilities to solve problems or tasks efficiently. So, ML is an enabler for AI. A high-level process of how AI and ML work together includes[27]:

1. An AI system is built using machine learning and other technique
2. Machine learning models are created by studying patterns in the data
3. Data scientists optimize the machine learning models based on patterns in the data
4. The process repeats and is refined until the models' accuracy is high enough for the tasks that need to be done

Some of the common use case for AI/ML on Azure includes:

- Predictive analytics
- Recommendation engines
- Speech recognition and natural language understanding
- Image and video processing
- Sentiment Analysis

Azure's cloud provides various AI and ML based offerings for media and entertainment industry which are worth exploring or adding on your organization's future development roadmap and strategy. Video Analyzer for Media (formerly known as Video Indexer) is one such example that extracts insights and metadata such as spoken words, faces, emotions, topics, and brands from media files. Some of the additional capabilities and improved model updates include functionalities like multilingual identification and transcription, extraction of people and locations entities, editorial shot detection model etc[28].

Details for Video Analyzer for Media (formerly known as Video Indexer) can be found here
Details for Azure Video Analyzer (formerly known as Video Analytics) can be found here

6.3 Passwordless

User authentication remains one of the key security controls that is usually in place to protect systems, application, and data from different types of identity attacks. Functionalities like multi-factor authentication (MFA) has been in play for a while now to add additional layer of defense against the different types of attacks that passwords are susceptible to. Whereas features like MFA does provide the additional security layer, it can become frustrating and inconvenient for the end user. Recent introduction of Passwordless technology might be a solution to this problem.

[27] https://azure.microsoft.com/en-gb/overview/artificial-intelligence-ai-vs-machine-learning/#introduction
[28] https://azure.microsoft.com/en-us/blog/azure-media-services-new-ai-powered-innovation/

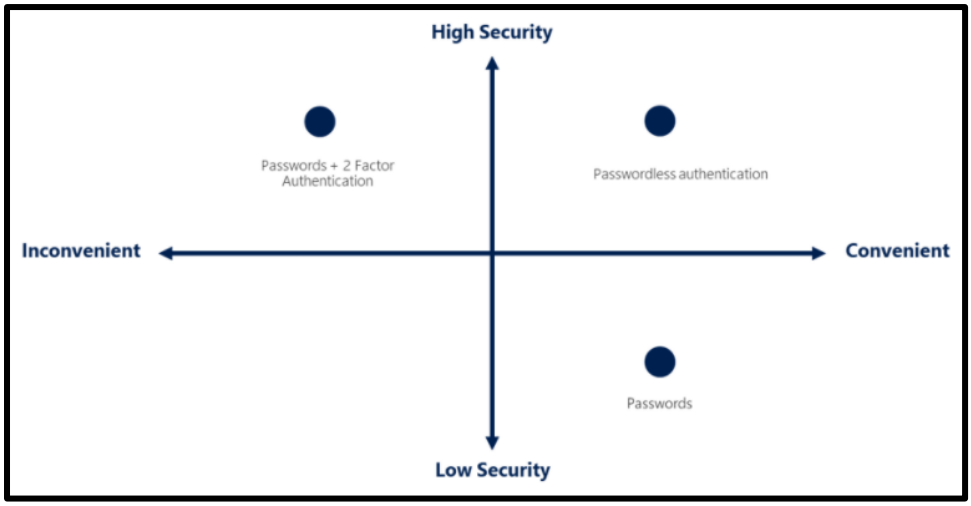

Figure 34 – Passwordless[29]

Passwordless is the process of verifying user identity without requiring user to provide a password. Instead, it depends on biometric verification and public/private key cryptography. Open standards like W3C WebAuthn and Fast Identity Online 2 (FIDO2) are enabling passwordless authentication across platforms using combination of authenticator devices and biometrics (fingerprint scanner, facial recognition etc.)[29].

Azure AD provides passwordless functionality in cloud using authentication methods like Windows Hello for Business, Microsoft Authenticator App and FIDO2 security keys. Additional details regarding use of passwordless on Azure are here and implementation details can be found here

[29] https://www.microsoft.com/en-gb/security/business/identity-access-management/passwordless-authentication

7. Appendices

7.1 Appendix A – Compliance Matrix

As part of this guide, Convergent have reviewed relevant compliance standards and architecture frameworks that are applicable to media and entertainment industry. These include:

- CIS
- CAIQ
- CDSA
- MPA
- MovieLabs ECPP
- MovieLabs Zero-Trust Architecture

Azure Security Best Practices were mapped to each of the controls from the respective compliance standards and controls framework. The details in this section can be used evaluate how your Azure cloud environment meets different compliance standards and controls framework requirements that are applicable to the media and entertainment industry.

7.1.1 Use Strong Network Controls

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Treat identity as the primary security perimeter	Azure AD Azure AD Connect	No	Not aligned but recommended	No	No	3.4.1	Security Architecture Pt1 -3.1
Centralize identity management	Azure AD Azure AD Connect Azure AD B2B & B2C	5.6, 6.7 & 12.5	No	No	05.17.1	Recommended Practice 6	Security Architecture Pt1 -5.1
Manage connected tenants	Azure AD	No	MS-12.5	No	No	No	No
Enable single sign-on	Azure AD	No	No	No	No	Recommended Practice 6	Security Architecture Pt1 -6.1
Turn on conditional access	Azure AD Conditional Access	No	No	No	No	No	No
Enable password management	Azure AD SSPR Azure AD Password Protection	5.2	DS-8.1	IAM-02.1	05.15.6	No	Security Architecture Pt1 -6.2
Enforce multi-factor verification for users	Azure AD Azure AD (Premium) Azure AD (P2) Azure Identity Protection	6.4 & 6.5	DS-8.1	No	No	No	No
Use role-based access control	Azure AD	6.1	MS-3.0	IAM-09.1	05.17.3	No	Security Architecture Pt1 - 5.3.1
Lower exposure of privileged accounts	Azure AD PIM MS Authenticator App Defender for O365 Attack Simulator O365 Activity Monitoring	No	No	IAM-09.1, IAM-09.2 and IAM-09.3	05.17.4	No	No

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Control locations where resources are created	Azure Resource Manager	No	No	DSP-19.1	No	No	No
Actively monitor for suspicious activities	Azure AD Premium Azure AD Identity Protection	13.3	DS-9.1	LOG-03.1	05.16.4	3.5	Security Architecture Pt1 -6.5
Use Azure AD for storage authentication	Azure AD	No	No	No	No	No	No

7.1.2 Lock down and secure VM and computer operating systems

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Protect VMs by using authentication and access control	Azure Management Groups Azure Policies Azure Resource Groups Azure Resource Manager Azure Roles	No	DS-8.0	No	No	No	Security Architecture Pt1 - 3.3
Use multiple VMs for better availability	Azure availability sets	12.1	No	No	No	No	No
Protect against malware	Microsoft Defender	10.1	DS-6.0	TVM-02.1	05.5.18	No	No
Manage your VM updates	Azure Automatic VM Patching Azure Backup Azure Marketplace	7.3, 7.4 & 16.4	DS-6.4	TVM-05.1	05.8.2	No	No
Manage your VM security posture	Defender for Cloud	16.2	DS-1.12 & DS-3.9	No	05.8.2	7.2.2	No
Monitor VM performance	Azure Monitor	No	No	No	No	No	No

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Encrypt your virtual hard disk files	Azure Disk Encryption Azure Key Vault Azure Backup Azure Key Vault	3.6	DS-6.7 & DS-11.0	UEM-08.1	05.11.11	7.2.1	Security Architecture Pt1 - 5.3.2
Restrict direct internet connectivity	Azure RBAC Defender For Cloud Azure Privileged Access Management	No	DS-2.0	No	05.6.10, 05.10.1 & 05.10.2	No	No

7.1.3 Protect Data

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Choose a key management solution	Azure Key Vault Azure RBAC	No	DS-11.5	No	5.24.16	No	Securing the Vision - Security Principle 5
Manage with secure workstations	N/A	12.8	No	No	No	No	No
Protect data at rest	Azure Disk Encryption	3.1	DS-6.7, DS-11.1 & DS-11.4	CEK-03.1	05.3.2, 05.6.12, 05.11.11 & 05.19.1	7.2.1	Security Architecture Pt1 - 5.3.2
Protect data in transit	Azure Site-to-site VPN Azure Point-to-site VPN Azure ExpressRoute Azure Portal Azure Storage REST API	3.11	DS-11.4	CEK-03.1	05.11.11 & 05.11.2	7.2.1	Security Architecture Pt1 - 5.3.2
Secure email, documents, and sensitive data	Azure Information Protection Usage Logging for Azure RMS	9.6, 9.7, 5.4, 3.12, 3.3	DS-2.0, DS-2.1, DS-15.11,	DSP-01.1	05.3.2, 05.6.12, 05.11.11 & 05.19.1	7.2.1	No

7.1.4 Secure Databases

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Use firewall rules to restrict database access	Azure Firewall Azure NSG's	13.1	No	No	No	No	No
Enable database authentication	Azure SQL Database Azure Key Vault	No	No	No	No	No	No
Protect your data by using encryption	Azure SQL TDE	No	DS-11.4	CEK-03.1	No	7.2.1	Security Architecture Pt1 - 5.3.2
Enable database auditing	Azure SQL Database	No	No	No	No	No	No
Enable database threat protection	Azure SQL Database Azure Defender for SQL Azure Defender for SQL	No	No	No	No	No	No

7.1.5 Define and deploy strong operational security practices

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Manage and monitor user passwords	Azure Active Directory Azure Directory Reports Azure Identity Protection	5.2	DS-7.2 & DS-8.1	IAM-15.1	05.11.6	Recommended Practice 5	No
Receive incident notifications from Microsoft	N/A	No	No	SEF-07.1	05.17.1, 05.17.2, 05.17.3, 05.17.4, 05.17.5, 05.17.6 & 05.17.7	Recommended Practice 13	No
Organize Azure subscriptions into management groups	Azure Management Groups	No	No	No	No	No	No
Streamline environment creation with blueprints	Azure Blueprints	No	No	No	No	Recommended Practices 16 & 17	No
Monitor storage services for unexpected changes in behavior	Azure Storage Analytics	13.3	DS-9.3	IVS-02.1	No	No	Security Architecture Pt1 - 6.5
Prevent, detect, and respond to threats	Microsoft Defender for Cloud Azure Sentinel Azure Secure Score Microsoft Defender for Cloud Azure Monitor Windows Defender ATP	13.1, 13.3 & 13.8	DS-9.1, DS-9.2, DS-9.3 & DS-9.4	IVS-09.1 & LOG-05.1	05.16.6	Recommended Practice 4	Security Architecture Pt1 - 6.5

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Monitor end-to-end scenario-based network monitoring	Azure Network Watcher Azure Flow Logs Azure Network Watcher	13.3 & 13.8	No	LOG-13.1	No	3.5	Security Architecture Pt1 - 6.5
Secure deployment by using proven DevOps tools	Azure Resource Manager Azure Pipelines Azure Application Insights	No	No	AIS-04.1	No	No	No
Mitigate and protect against DDoS	Azure Secure Development Lifecycle Azure App Service Azure Virtual Machines Azure Virtual Machine Scale Sets Azure Load Balancer Azure Application Gateway Network Security Groups Azure Service Tags Application Security Groups Azure Service Endpoints Azure DDoS Protection	No	No	No	No	3.3.2	No
Enable Azure Policy	Azure Policy	No	No	No	No	No	No
Monitor Azure AD risk reports	Azure AD Risk Reports	No	No	No	No	Recommended Practice 13	No

7.1.6 Design, build, and manage secure cloud applications

Azure Security Best Practice	Azure Service Enabling	CIS v8.0	TPN / MPA v4.10	CAIQ/CCM v4.03	CDSA	MovieLabs ECPP	MovieLabs Zero Trust
Adopt a policy of identity as the primary security perimeter	Azure Key Vault Azure MFA Azure MFA	No	No	No	No	3.4.1	Securing the Vision Section 1 - Introduction
Use threat modelling during application design	Microsoft SDL Azure Threat Modelling Tool	16.4	No	TVM-01.2	No	Recommended Practice 4	No
Develop on Azure App Service	Azure Active Directory Azure Active Directory RBAC Azure Key Vault Azure App Service Microsoft Defender for Cloud	No	No	No	No	No	No
Install a web application firewall	Azure Web Application Firewall	13.10	No	No	No	Recommended Practice 8	No
Monitor the performance of your applications	Azure Application Insights	No	No	IVS-02.1	No	No	No
Perform security penetration testing	N/A	16.3	DS-1.9	TVM-06.1	05.5.3	3.6	No

END OF REPORT