avanade

SFTP Security Design & Recommendations for Colonial First State

Ref. - Security Architecture (FR09, FR10 and FR11)

Version History			
Version #	**Revision Date**	**Author(s)**	**Change Description**
0.1	19/01/2023	Arnav Sharma	Initial Draft

Table of Contents

1. Introduction

The CFS team has engaged Accenture to work alongside the client and project teams to create a secure reference architecture for the Azure SFTP Solution.

Avanade will leverage our cloud security reference architecture as a baseline and understand the current setup, thereby providing detailed executable strategies/leading practices and cloud security key recommendations that will provide guidance and can be used by the Data Migration team as a model/reference for securing the solution.

The audience for this document is technical resources responsible for data migration using various Azure resources.

1.1. Purpose of the Document

This cloud security reference architecture aims to define a plan for implementing security practices to mitigate risks associated with Azure cloud computing effectively. The security reference architecture document will include architectural diagrams, detailed executable strategies/leading practices and cloud security key recommendations.

This design document covers the following critical areas for the SFTP services:

- Network and Endpoint Security
- Secure Storage
- Compute Security
- DevOps and Security Operations
- Key Management
- Security Monitoring and Alerting
- Vulnerability Management
- Malware Protection

1.2. Scope of the Project

- Identify client security requirements, solution components
- Define applicable security control for the solution components by applying the Secure by Design principle as per client security, compliance requirements
- Liaisethe with CFS Security team on identified security controls for approvals
    - Include security baseline in the detailed design document
    - Provide guidance to implement identified security controls in alignment with Security architecture
    - Review whether identified security controls are implemented adequately
    - Define the Process for deviation from the security baseline

1.3. Glossary of Terms

Acronym	TermInfrastructure as A Service
Iaas	Infrastructure as A Service
PaaS	Platform as A Service
SaaS	Software as A Service
NSG	Network Security Group
VPN	Virtual Private Network
RG	Resource Group

1.4. Key Decisions and Important Note References

Throughout this document, text boxes are used to draw attention to an important note or technical design decision or to highlight a decision that must be made to enable decision confirmation. The following is a key to these tables:

Note

Describes any important information

Recommendation

Describes any important recommendation.

Assumption

Describes any important assumption.

Requirement

Describes important requirement

Business Decision Required

Describes important decision

Critical Note

Describes important critical note

Decision

Describes essential decision has been made

2. Identity and Access Management

2.1 Subscription, Resource Groups & RBAC

2.1.1. Subscription

Subscription is a billing container that also serves as a security boundary and defines many Azure limits (e.g., number of cores and resources, etc.). Contains and organises all resources and establishes governance principles over them.

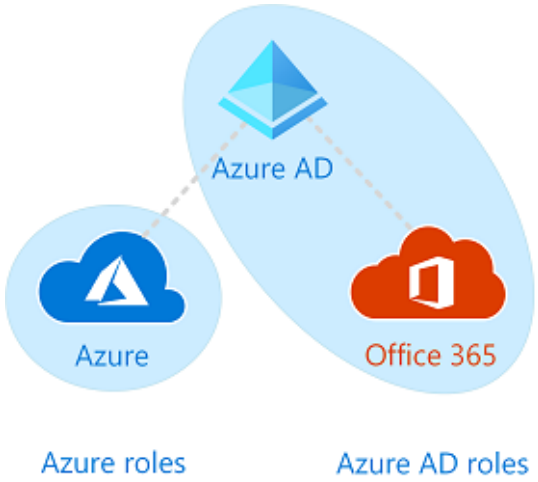
There are 3 main types of subscriptions available - free, pay-as-you-go, and member offers.

- The free account is a subscription that provides unlimited access to Azure resources with a $XXX credit that can be applied to paid products. At the end of the trial period, any Azure services created with the subscription are disabled, unless the subscription is upgraded to a paid subscription. Free accounts require a credit card, used for identification purposes only.
- The pay-as-you-go subscription lets you pay for the services and resources that you use on a monthly basis. A credit or debit card must be attached to the account and billing for this account is on a monthly basis. Free Azure accounts can be converted to pay-as-you-go accounts.
- There are many types of member offers that provide reduced rates for Azure services, like MSDN Platform subscribers and Visual Studio subscribers just to name a few. These types of subscriptions offer substantial discounts over a pay-as-you-go subscription, so it is highly recommended that businesses review and take advantage of any offers for which they may qualify.

2.1.2. Resource Group

Azure Resource Groups are logical containers within a subscription that contain related Azure resources sharing a common lifecycle. Azure Resource is a logical container that groups multiple resources together. Every resource that you create inside Azure must belong to a resource group. An example would be Application Spoke Resource Groups that share the same life cycle (prod, non-prod) resource, like virtual machine, SQL Server and Database, Storage, etc. and grouped inside the same resource group. They can then be managed and deleted as a single entity.

2.1.3. Role Based Access Control (RBAC)



As shown above Azure AD provides RBAC for both Azure and Office 365 user roles. Because Azure AD supports Office 365 and Azure in the same directory – when considering when to create additional Azure Tenants, it is recommended to isolate customer identities form Corporate identities. E.g, client should be in a separate tenant from Customer facing application such as a PAM.

2.1.4. Azure Resource Roles

Azure RBAC has approximately 221 built-in roles that you can use to manage Azure Resources, by assigning users, groups, service principles and manage identities. The following Azure Services categories have built-in Roles that will be leverage for the initial deployment of Middle Office and PAM application as of this writing:

Categories of Built-in Roles

- General
- Compute
- Networking
- Storage
- Web
- Containers
- Databases
- Analytics
- Integration
- Identity
- Security
- DevOps
- Monitor
- Management + governance
- General
- Compute
- Networking

The full list of built-in Azure Resource Roles are maintained here: Azure built-in roles - Azure RBAC | Microsoft Docs

2.1.5. RBAC boundaries

When defining RBAC roles and membership into those roles, there are 2 key areas to understand and define.

- Subscription RBAC
- Resource Group RBAC

Subscription-based RBAC is one of the top levels RBAC boundaries. RBAC roles are inherited, meaning if subscription-level access is granted, then the user will have access to all resources in the subscription

based on the subscription level role they were assigned. The subscription-based access is highly restricted. Typically, most users are granted access on a resource group level. Reasons when a user would need subscription based RBAC access would be primarily for administrative based tasks. Normal application team users will not have subscription-based access.

Resource Group RBAC assignment is where most of RBAC assignments will be made. Resource groups will be logically grouped so that they contain resources belonging to a specific application. With this resource group organization, teams can get proper access to only their resources while protecting the rest of the Azure subscription and other resources.

Recommendation:

- Existing Subscriptions / Resource Group to be used.
- CFS is responsible for managing access to SFTP resources.
- Access control should be managed on Resource Group level.

Note:

- IAM is not a part of the current scope

2.2. Managed Identity

Managed identity - an identity in Azure Active Directory that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage credentials for authenticating to Azure services.

In Azure AD, you will need a directory object (Object ID) to manage any identity (users, applications, groups etc.). In that context, Azure needs a directory object for managing the managed identities as well.

Managed identity provides Azure services with an automatically managed identity in Azure Active Directory and is used to authenticate to any service that supports Azure AD authentication, without having credentials in your code.

Managed identities types:

- System-assigned: These identities are tied directly to a resource and abide by that resources' lifecycle. For instance, if that resource is deleted then the identity too will be removed
- User-assigned: These identities are created independent of a resource, and as such can be used between different resources. Removing them is a manual process whenever you see fit

One of the problems with managed identities is that for now only a limited subset of Azure services support using them as an authentication mechanism. If the service you use doesn't support MI, then you'll need to either continue to manually create your service principals.

2.2.1. What Do Managed Identities Not Do?

Inbound requests: One of the biggest points of confusion about Managed Identity is whether they are used for inbound requests to the resource or for outbound requests from the resource. Managed Identities are for the latter – when a resource needs to make an outbound request, it can identify itself with a Managed Identity and pass its identity along to the resource it's requesting access to.

Managed Identity pair nicely with other features of Azure resources that allow for Azure AD tokens to be used for their own inbound requests. For example, Azure Key Vault accepts requests with an Azure AD token attached, and it evaluates which parts of Key Vault can be accessed based on the identity of the caller. Managed Identity can be used in conjunction with this feature to allow an Azure resource to directly access a Key Vault-managed secret.

2.2.2. Authorization

Another important point is that Managed Identity are only directly involved in authentication, and not in authorization. In other words, a Managed Identity allows Azure AD to determine what the resource or application is, but that by itself says nothing about what the resource can do. For some Azure resources this is Azure's own Identity and Access Management system (IAM). Key Vault is one exception – it maintains its own access control system and is managed outside of Azure's IAM. For non-Azure resources, we could communicate with any authorization system that understands Azure AD tokens; a Managed Identity will then just be another way of getting a valid token that an authorization system can accept. Another important point to be aware of is that the target resource doesn't need to run within the same Azure subscription, or even within Azure at all. Any service that understands Azure Active Directory tokens should work with tokens for Managed Identity.

2.2.3. Managed Identity vs. Service Principle

Is it always recommended to use Managed Identities in Azure, mostly system assigned or a Service Principal? When should Service Principals be used in Azure compared to managed identity, what is the advantage of one over the other?

Internally, managed identities are service principals of a special type, which are locked to only be used with Azure resources. When the managed identity is deleted, the corresponding service principal is automatically removed. Also, when a User-Assigned or System-Assigned Identity is created, the Managed Identity Resource Provider (MSRP) issues a certificate internally to that identity.

Recommendation:

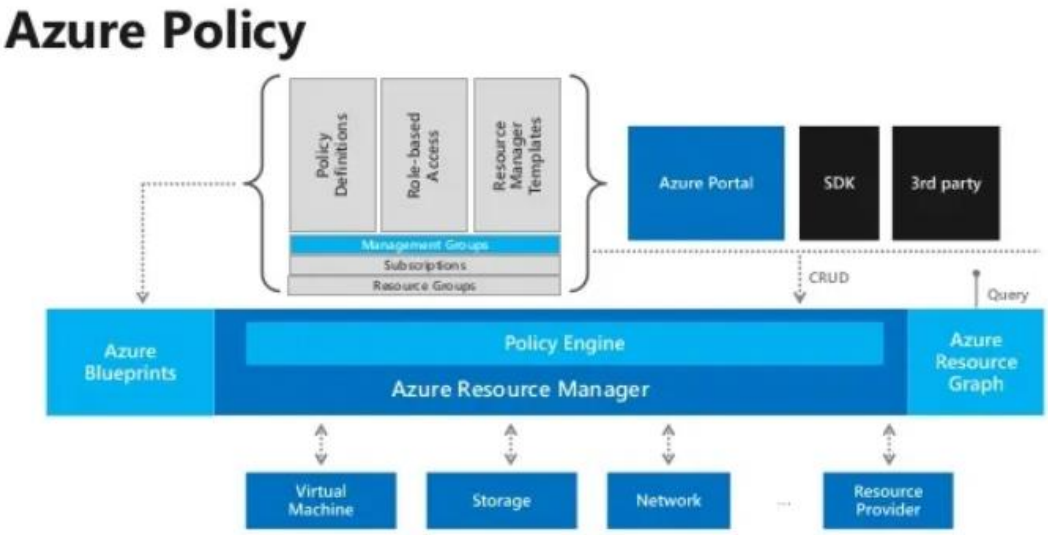
- Use managed identity for authentication for resource authentication.
- No username / password to be hardcoded on the application side.

Note:

- IAM is not a part of the current scope

3.Governance and Policy Drift – Azure Policy

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different 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. Once a policy is implemented, new and existing resources are evaluated for compliance.



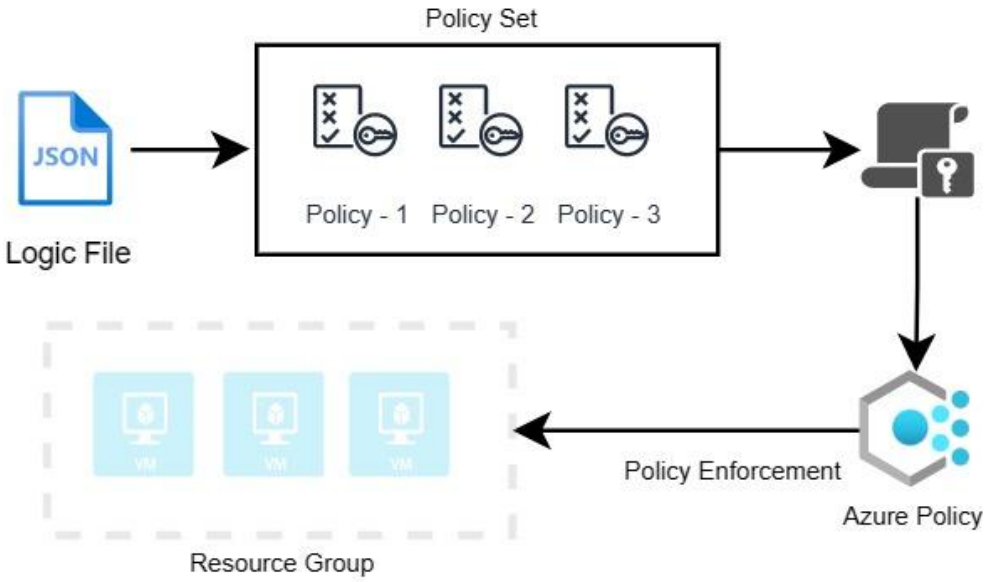
Azure Policy evaluates resources and actions in Azure by comparing the properties of those resources to policy definitions. Azure Policy uses a JSON format to form the logic the evaluation uses to determine whether a resource is compliant or not. Azure Policies can be applied at the Management Group, Subscription, or Resource Group scope.

Resources are evaluated at specific times during the resource lifecycle, the policy assignment lifecycle, and for regular ongoing compliance evaluation

Azure Policy Objects:

- Policy definition – Creating and implementing a policy in Azure Policy begins with creating a policy definition.Every policy definition has conditions under what it's enforced and defined effect takes place if the policy is met.
- Initiative definition – It's a collection of policy definitions that are tailored toward achieving a singular overarching goal.
- Assignments - An assignment is a policy definition or initiative that has been assigned to a specific scope. This scope could range from a management group to an individual resource.

3.1.1 VM Governance using Azure Policy



The requirement here is to ensure that the VM's and storage account always have the Defender enabled.

- Defender for Cloud agent in integration with Defender for Endpoint will check for Malware and viruses on the VM instance.
- Defender for Storage will ensure that there are no attacks or malware threats on the storage accounts.

✓	**Recommendation:**
	• Policies to be enforced:
	  ○ Configure supported Windows machines to automatically install the Azure Security agent
	  ○ Deploy Advanced Threat Protection on storage accounts
	  ○ Deploy Microsoft Defender for Endpoint agent on Windows virtual machines
	• Policies to be set to – Deploy if not exists.

4 Malware Scanning

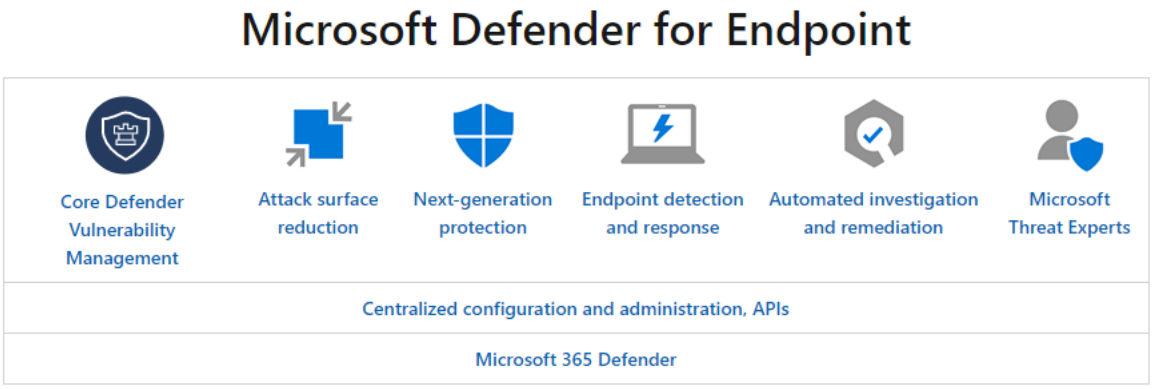
Malware or “malicious software”, is an umbrella term that describes any malicious program or code that’s harmful to systems.Malware can reveal itself with many different aberrant behaviours such as system slowness, system crash or loss access to files.

Malware scan tools helps to search for any files or programs on systems that can harm it. A malware scan is as effective as its last definition update, which means if it is not updated regularly it may be unaware of and unable to detect newer forms of malware.

4.1.1 Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

We can apply for the Microsoft Threat Experts managed threat hunting service to get proactive Targeted Attack Notifications and to collaborate with experts on demand. Experts on Demand is an add-on service. Targeted Attack Notifications are always included after you have been accepted into Microsoft Threat Experts managed threat hunting service.



- Core Defender Vulnerability Management is the built-in core vulnerability management capabilities use a modern risk-based approach to the discovery,assessment and remediation of endpoint vulnerabilities and misconfigurations.
- Attack surface reduction provides the first line of defence in the stack.
- Next-generation protection is to further reinforce the security perimtere of your network.
- Endpoint detection and response capabilities are put in place to detect,investigate and respond to advanced threats.
- Automated investigation and remediation is to quickly respond to advanced attacks,Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that helpreduce the volume of alerts in minutes at scale.
- Microsoft Secure Score for Devices is to dynamically assess the security state of enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of organization.
- Centralized configuration and administration,API’s is to integrate Microsoft defender for Endpoint into existing workflows.

- Microsoft 365 Defender, Defender for Endpoint, and various Microsoft security solutions, form a unified pre- and post-breach enterprise defense suite that natively integrates across endpoint, identity, email, and applications to detect, prevent, investigate, and automatically respond to sophisticated attacks.

4.1.2 Scan Schedule & Actions

A malware scan configuration specifies what types of malware scanning Deep Security will perform and which files it will scan. You can set up multiple malware scan configurations to suit your needs.

There are two kinds of malware scan configurations: **Real-time Scan** and **Manual/Scheduled Scan**. While most actions are available to both types of scans, some actions, like Deny Access are available to Real-time Scans only, and other options, like CPU Usage are available to Manual/Scheduled Scans only.

In addition to always-on, real-time protection and on-demand antivirus scans, you can set up regular, scheduled antivirus scans. You can configure the type of scan, when the scan should occur, and if the scan should occur after a protection update or when an endpoint isn't being used. You can also set up special scans to complete remediation actions if needed.

✓	**Recommendation**: Malware Scanning • Realtime scanning enabled. • Auto remediation enabled. • Full System Scan after business hours.

4.1.3 Integrating Defender for Cloud and Defender for Endpoint

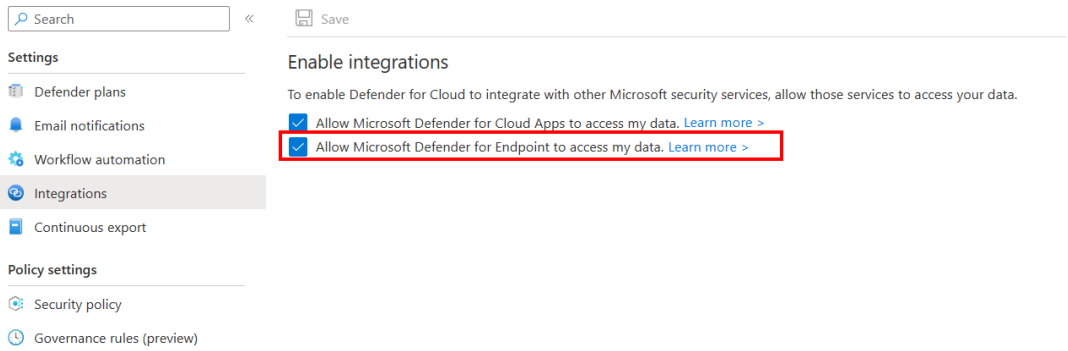
Microsoft Defender for Endpoint protects your Windows and Linux machines whether they're hosted in Azure, hybrid clouds (on-premises), or multi-cloud environments.

The protections include:

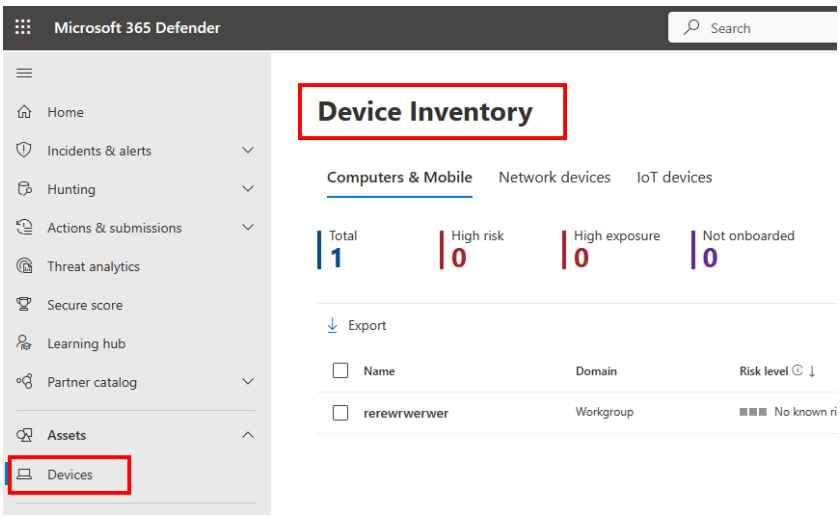
- Advanced post-breach detection sensors. Defenders for Endpoint's sensors collect a vast array of behavioral signals from your machines.
- Vulnerability assessment from the Microsoft threat and vulnerability management solution. With Microsoft Defender for Endpoint installed, Defender for Cloud can show vulnerabilities discovered by the threat and vulnerability management module and also offer this module as a supported vulnerability assessment solution. Learn more about investigating weaknesses with Microsoft Defender for Endpoint's threat and vulnerability management.
- Analytics-based, cloud-powered, post-breach detection. Defender for Endpoint quickly adapts to changing threats. It uses advanced analytics and big data. It's amplified by the power of the Intelligent Security Graph with signals across Windows, Azure, and Office to detect unknown threats. It provides actionable alerts and enables you to respond quickly.

- Threat intelligence. Defender for Endpoint generates alerts when it identifies attacker tools, techniques, and procedures. It uses data generated by Microsoft threat hunters and security teams, augmented by intelligence provided by partners.

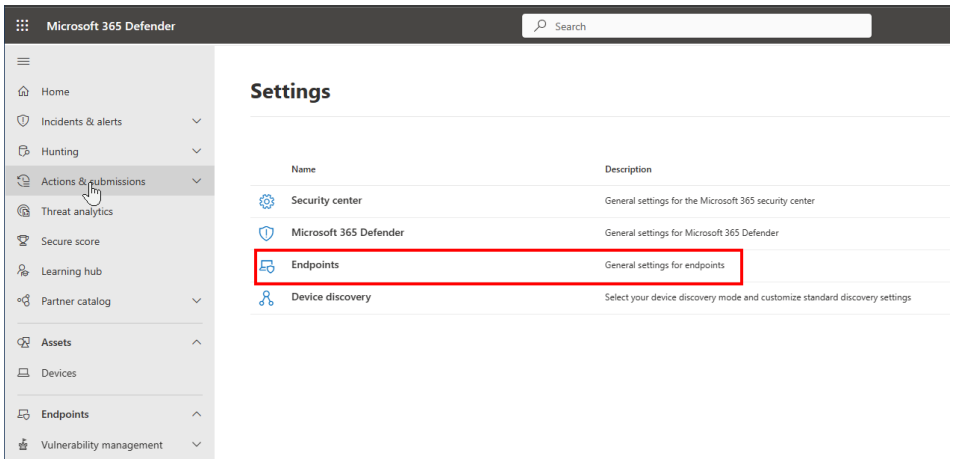
Integrating the Defender for Cloud with MDE from Azure Portal:



The devices onboarded to MDE will show up in the Security Dashboard:



Malware Scanning can be customised using https://security.microsoft.com/



✓	**Recommendation**: • Integrate MDE with Defender for Cloud • Ensure the validation of Azure VM's in MDE Console, under device Inventory. • Configure the scans as per the recommendation in previous section.

4.1.4 Defender for Storage Accounts.

Azure-native security - With one-click enablement, Defender for Storage protects data stored in Azure Blob, Azure Files, and Data Lakes. As an Azure-native service, Defender for Storage provides centralized security across all data assets managed by Azure and is integrated with other security services such as Microsoft Sentinel.

Rich detection suite - Powered by Microsoft Threat Intelligence, the detections in Defender for Storage cover the top storage threats such as anonymous access, compromised credentials, social engineering, privilege abuse, and malicious content.

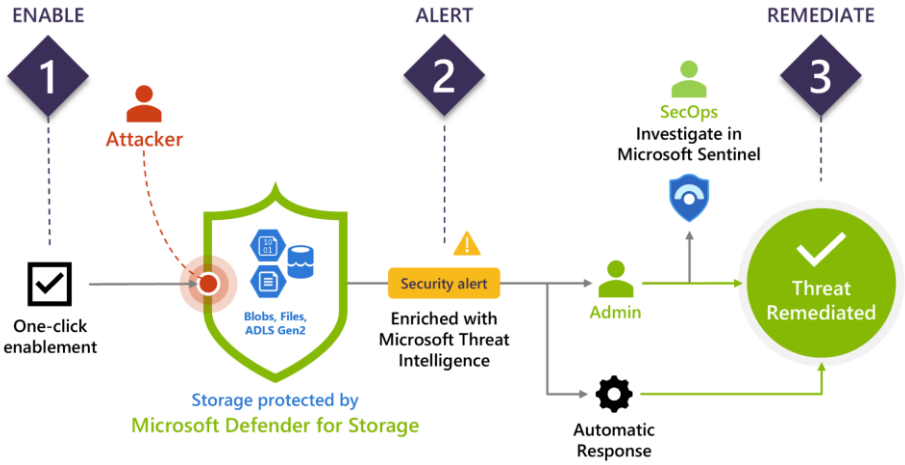
Response at scale - Defender for Cloud's automation tools make it easier to prevent and respond to identified threats. Learn more in Automate responses to Defender for Cloud triggers.

Security alerts are triggered when there are:

Suspicious access patterns - such as successful access from a Tor exit node or from an IP considered suspicious by Microsoft Threat Intelligence

Suspicious activities - such as anomalous data extraction or unusual change of access permissions

Uploads of malicious content - such as potential malware files (based on hash reputation analysis) or hosting of phishing content



Recommendation:

- Configure the Azure Policies as per section 3.1.1
- Ensure the storage account is reported in Defender for Cloud.
- Configure the scans as per the recommendation in previous section.
- Ensure that Azure Monitor is set to correct Alerting / Action Group. (For email alerts)

Note:

- Azure Monitor configuration is not in current scope.
- Alerting to be setup by existing team.

4. Network & Endpoint Security

4.1. Virtual Network & vNET Peering

Azure Virtual Network (vNET) is a logically isolated network in Azure. Each Azure vNET runs on same underlying shared physical network infrastructure however they are fully isolated from each other. Azure Networking stack uses VXLAN technology underlying to facilitate all these.

vNET is the foundation of customer's infrastructure in Azure cloud, you would require planning and design vNET before you deploy any resources in Azure because it's the VNET that will facilitate network communication for the resources deployed within Azure VNET.

vNET is a fundamental building block for your private network with features/properties that provide horizontal scaling and isolation:

- Subnets – provide segmentation capability of your vNET by slicing vNET into subnets and allocate portion of addresses into each subnet

- Peering – allows to connect vNET to vNET and resources from one vNET to communicate with other vNET resources

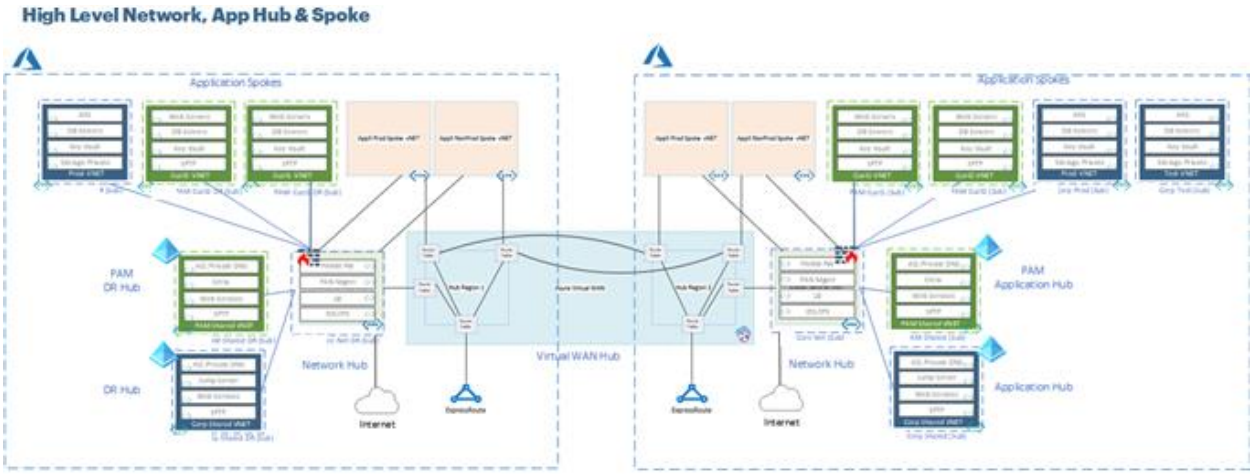
- vNET Service endpoint - extends your vNET private address space to Azure service resources over the direct connection. Example would be Azure SQL with Firewall Rules over a direct connection.

- vNET Private Link – an Azure service that enables customers to access supported Azure PaaS Services (Azure SQL, Key Vault, Event Hub, Storage etc..) over a private endpoint in an Azure Virtual Network. This ensures the network traffic between virtual network and service travels via the Microsoft backbone within your network boundary, including from on-premises when connectivity such as ExpressRoute is configured.

- Allowing services to be addressable via a private IP address allows public IP addresses and therefore internet traffic to be blocked.

- It is also possible to create a Private Link Service in your virtual network and deliver it privately to your customers – Snowflake connectivity would be good use case here.

- Express Route – private connection (over MSFT backbone/internal network and 3rd party MPLS circuit provider) between your on-premise network and Azure. With express route traffic does not go over the internet



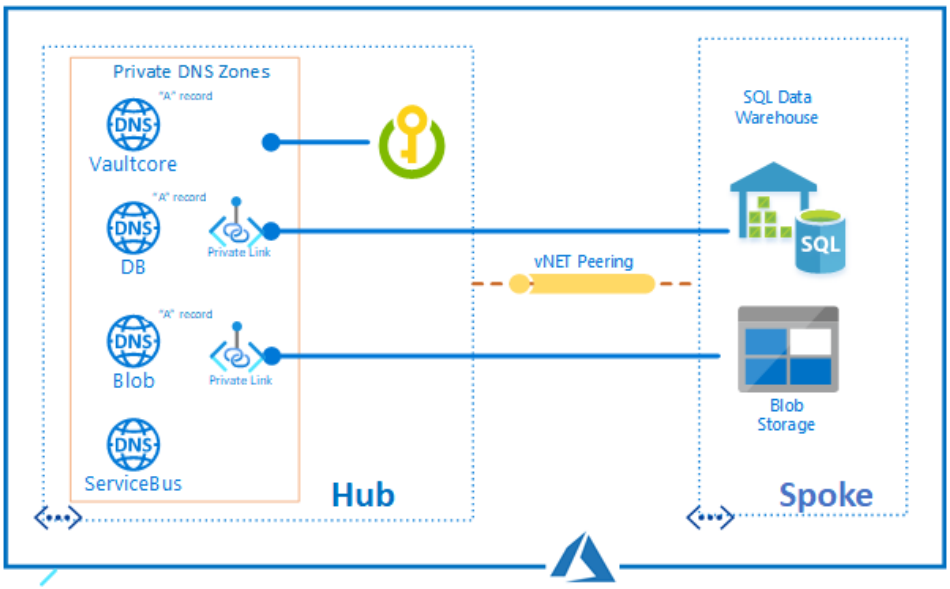
✓	**Recommendation:** • CFS is using Hub and Spoke Topology. • All the spoke vNET's are peered with Hub Subnet only. • All the traffic should be routed via Hub vNET. • No additional peering should be done.

4.2. SFTP Endpoint

SFTP is a platform level service, so port 22 will be open even if the account option is disabled. If SFTP access is not configured, then all requests will receive a disconnect from the service. When using SFTP, you may want to limit public access through configuration of a firewall, virtual network, or private endpoint. These settings are enforced at the application layer, which means they aren't specific to SFTP and will impact connectivity to all Azure Storage Endpoints.

4.3. Storage & Keyvault Endpoint

Azure Private Endpoints is a network interface that connects you privately and securely to a service powered by Azure Private Link. The Private Endpoint uses a private IP address from your VNet that brings the service into your vNet. However, the service could be an Azure service like Storage, Cosmos DB, SQL, etc. or your own Private Link Service.



7.1.1 Key details about Azure Private Endpoint

It enables connectivity between the consumers from the same vNET and on-premises using VPN or Express Route and services powered by Private Link.

Network connections can only initiate by clients connecting to a Private endpoint.

while creating a private endpoint, a read-only network interface is also created for the lifecycle of the resource. The interface is for private IP addresses from the subnet that maps to the private link resource. But, the value of the private IP address remains unchanged for the entire lifecycle of the private endpoint.

Private endpoint deployment must be in the same region as the virtual network. But the private link resource deployment can be in a different region than the virtual network and private endpoint.

Multiple private endpoints can be created using the same private link resource. Also, the multiple private endpoints can be created on the same or different subnets within the same virtual network. As there are limits to the number of private endpoints you can create in a subscription.

✓	**Recommendation:** • KeyVault and Storage account should use endpoints only. • No public endpoint to be exposed for either of the resources.

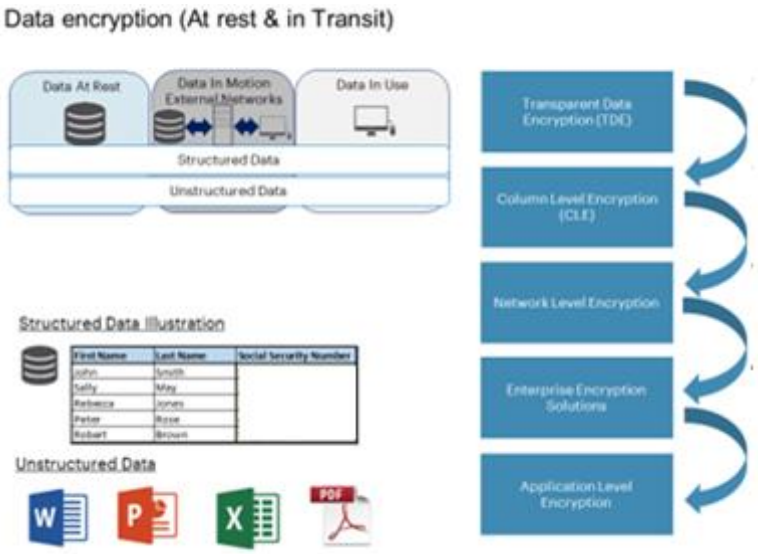
5.Secure Storage

5.1. Encryption

Data Protection ensures that sensitive data is protected based on the classification and not compromised outside the enterprise.

- Data Masking is the obfuscation of data on an as-required basis to fulfill regulatory needs and prevent unauthorized access to sensitive data (e.g. screens containing multiple fields, with some obfuscated).
- Data Anonymization is the removal of identity from data as it is transferred or processed. Includes reversible, pseudo-random and random approaches depending on requirement.
- Data Encryption at Rest services cover encryption of data at rest in storage and/or database (i.e. encryption at the physical or virtual layer).
- Data In Transit Protection counteracts data tampering and eavesdropping through a combination of network protection and encryption. This protection should be between end user devices and the service, internally within the service and between the service and other services. It can be implemented using private WANs, SSL/TLS and IPsec VPN Gateways.

Following are At rest and in transit data encryption methods :



8.1.1 Transparent Data Encryption

Transparent Data Encryption: Method where you can encrypt entire database but don't have to change many of the applications that access it. Focus on data at rest. Decrypted when you "read" the database

8.1.2 Column Level Encryption

Column Level Encryption: Data that can be encrypted at the column. Also known as cell level encryption. Provides protection for data in motion via disk or even memory until decrypted typically at the application level. Available with Oracle and SQL enterprise solutions

8.1.3 Network Level Encryption

Network Level Encryption: Data that requires encryption in motion and in use. This is the standard point to point VPN, SSL or SSH channel. Can be useful for high transaction applications sharing sensitive information between third parties. Easier than complete customization

8.1.4 Enterprise Encryption Solutions

Enterprise Encryption Solutions: Various solutions that provide different levels of encryption from masking to tokenization. Provide format preserving capabilities for easier encryption methods. Includes Dynamic and Persistent capabilities

8.1.5 Application Level Encryption

Application Level Encryption: This is the process of encrypting data at the application level before it is stored in the database. One of the most secure methods but difficult to implement and maintain

8.1.6 Azure Encryption in Transit

Network traffic within the Azure Virtual Network and ExpressRoute circuits is not encrypted, each application is required to address the encryption in transit requirements and implement a suitable solution that meets Client's Cyber Security requirements and seek endorsement. Data leaving the client's virtual network should be considered unsecure and so appropriate safeguards such as HTTPS or VPN will be implemented in accordance with client's existing methods. In addition, when interacting with Azure Portal, REST API, or PowerShell communications will be encrypted in transit.

Recommendation: **Encryption in Transit**

- Each application is required to address the encryption in transit requirement.

8.1.7 Azure Encryption at Rest

Client will have control to decide when data needs to encrypt, encryption keys used and where they are stored and can decide at any time to revoke access to the keys for data at rest.

Azure offers full transparency to the encryption state of the data at rest. Client will have the full control of where the data is stored which will enable compliance with geographic laws. Client can setup configure monitoring and alerting of the data at rest which will give the capability to view the logs for the stored data and keys.

Server Encryption Model, Encryption Keys are managed by the azure server service. In this case Azure will be able to see the decrypted data. For server-side encryption client can bring own encryption key and Azure will manage client key within their HSM solution.

Client encryption model, client will manage the security of the keys, encryption methods, but comes at a reduced cloud functionality due to client managing every aspect rather than leveraging Azure services.

Encryption at the Azure Storage infrastructure level: When infrastructure encryption is enabled, data in a storage account is encrypted twice , once at the service level and once at the infrastructure level with two different encryption algorithms and two different keys

Encryption at rest for Operating System and Data Disks will be implemented by BitLocker at the Volume level on all OS and Data disks. To facilitate the encryption of the host OS and Data disks, the Azure Disk Encryption VM extension will be used to provide native BitLocker functionality and Key Management. The Azure Disk Encryption VM extension enables the BitLocker Windows feature and facilitates the uploading of the BitLocker Encryption Key into the Azure Key Vault. Key Vault is a Microsoft hosted Key Management provider that can be leveraged to store encryption keys.

Note

- Data Access Controls - Controls for data access via the Azure's management plane, Controls for public and internal data sharing and controls for application level data access.
- Data Classification - Classification of data type, Data Owner and risk under the confidentiality, availability and Integrity buckets as directed by reputable standards organizations like NIST, ISO
- Data Encryption & Tokenization - Management of secure storage of data, encryption engine and the key management

Recommendation: **Encryption at Rest**

- Azure has multiple layers of encryption at rest, including the VM Managed Disk, and Storage Accounts. Its recommended to enable Encryption at Rest for all the resources.
- Additional details will be provided for specific resources modules in this document.

5.2. Azure Blob

Azure Blob Storage is a massive storage to contain large amounts of unstructured object data, like object or text data. It is mainly used for serving images to a browser, storing files for distributed access, streaming video and audio, backup and restore and mainly for data storage and analysis by another Azure service.

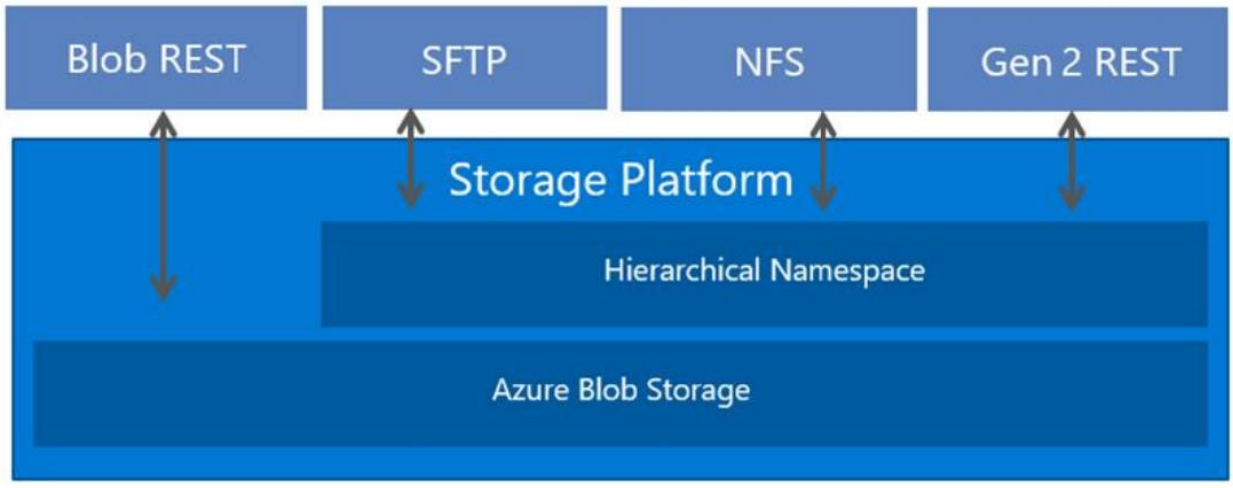
8.3.1 Azure File Storage

Azure File Storage - Azure File Storage provides shared storage using Server Message Block (SMB) and Common Internet File System (CIFS) protocols. In Windows file share, clients can add directory structures and files to the share and Azure File shares can be mounted to different Operating systems like Windows, Linux and MacOs.

8.3.2 Blob SFTP

Azure allows secure data transfer to Blob Storage accounts using Azure Blob service REST API, Azure SDKs, and tools such as AzCopy. However, legacy workloads often use traditional file transfer protocols such as SFTP. You could update custom applications to use the REST API and Azure SDKs, but only by making significant code changes.

With SFTP support for Azure Blob Storage, you can enable an SFTP endpoint for Blob Storage accounts with a single click. Then you can set up local user identities for authentication to connect to your storage account with SFTP via port 22.



8.3.3 Azure Table Storage

Azure Table Storage – is a NoSQL data storage

8.3.4 Azure Queue Storage

Azure Queue Storage – in a nutshell, an azure queue storage is a temporary storage of messages. I say temporary because if you don't act on a message within a certain time, the system automatically deletes the message. Currently, the default message live time is 7 days

8.3.5 Data Lake Gen 2

Azure Data Lake Storage (ADLS) is a fully managed, elastic, scalable and secure file system designed for big data analytics solutions. ADLS includes hierarchical file system with granular security and tiered storage along with processing capabilities, HA and DR. With a true hierarchical namespace to Blob storage, ADLS Gen2 allows true atomic directory manipulation.

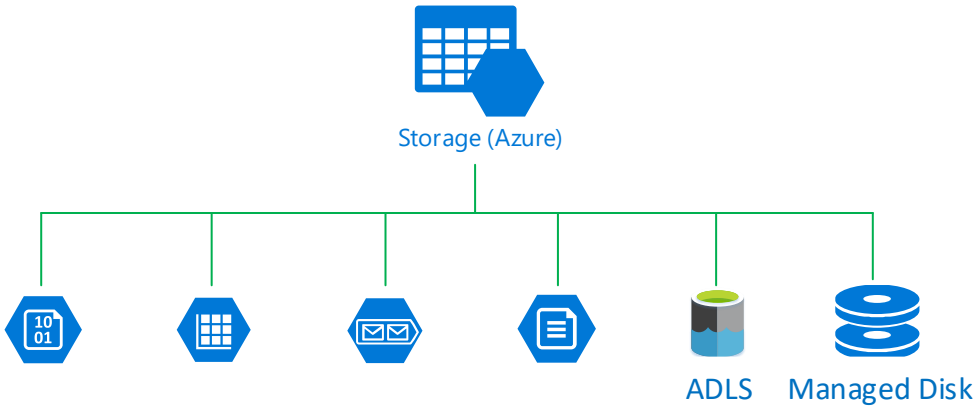
Data Lake Storage Gen2 makes Azure Storage the foundation for building enterprise data lakes on Azure. Designed from the start to service multiple petabytes of information while sustaining hundreds of gigabits of throughput, Data Lake Storage Gen2 allows you to easily manage massive amounts of data.

A fundamental part of Data Lake Storage Gen2 is the addition of a hierarchical namespace to Blob storage. The hierarchical namespace organizes objects/files into a hierarchy of directories for efficient data access. A common object store naming convention uses slashes in the name to mimic a hierarchical directory structure. This structure becomes real with Data Lake Storage Gen2. Operations such as renaming or deleting a directory, become single atomic metadata operations on the directory. There's no need to enumerate and process all objects that share the name prefix of the directory.

8.3.6 Azure Managed Disks

Azure Managed Disks are block-level storage volumes configured with virtual machines and managed by Azure. When you select managed disk, you just need to specify the disk size, the disk type, and provision the disk. Once you provision the disk, Azure handles the rest.

Features	Managed Disks	Unmanaged Disks
Management	Is an ARM (Azure Resource Manager) object (resource)	Is a file (.vhd) residing on an Azure Storage Account.
Size	disks sizes are fixed (and can be resized). Which means that you cannot choose a custom size.	Can choose the disk size during the provisioning (and can be resized) when using Standard Storage.
Performance	Has a predictable performance, with standard HDD, with Standard SSD storage, Premium SSD storage, Ultra Disk offering	Only premium storage disks have a predictable performance. Standard storage has a predictable performance (500 IOPS) unless they are impacted by the Storage Account performance limits
Availability	When placing Azure VMs using managed disks under an Availability Set, disks are placed on different fault domains in order to achieve the better SLA	When placing Azure VMs using unmanaged disks under an Availability Set, there is no guarantee that disks are placed on different fault domains, even if they are on different Storage Accounts.
Redundancy	Locally Redundant Storage (LRS)	LRS, GRS (Geo-redundant storage)



✓	**Recommendations** • Disable public access and enforce Private endpoint • Allow trusted Microsoft services to access the storage account • Enable FW rules • vNET service tags – service tag represents CIDRs prefixes from given Azure service. • Turn on point-in-time restore for containers • Turn on soft delete for blobs, containers and shares • Enforce HTTPS when a client uses a SAS token to access blob data • Secure transfer (HTTPS) • Enforce minimal TLS version • AAD to authorize access to blob data • Least privileges to Service Principle • User delegation SAS to grant limited access to blob data to clients • Disable Anonymous public read access to containers and blobs • Store Storage account access key in Azure Key Vault • Enable Azure Storage logging • Deploy Azure Security Policies to enforce Compliance requirements

8.3.7 Azure Files SMB

Azure File Sync is a cloud service that allows to keep aligned one or more folders between different servers in different locations. The Azure File service gives you a fully managed cloud file share and extends the ability of organizations to share files across on-premises and the cloud.

In this case the role of Azure is to orchestrate between each endpoint with the benefit to preserve ACLs. Furthermore, Active Directory is not required, and the solution works also in Workgroup (amazing for some scenarios).

All the information can be accessed via local SMB share, via Work Folders but also via remote SMB share. Indeed, all the files are stored into Azure File Share. Azure File Sync provides:

- Multi-site access – provide write access to the same data across Windows servers and Azure Files
- Cloud tiering – store only recently accessed data on local servers
- Integrates with Azure backup – no need to back up your data on premises
- Fast disaster recovery – restore file metadata immediately and recall data as needed

Note:

Some Limitations:

- Storage Sync Services per region: 100 Storage Sync Services
- Sync groups per Storage Sync Service: 200 sync groups
- Registered servers per Storage Sync Service: 99 servers
- Cloud endpoints per sync group: 1 cloud endpoint
- Server endpoints per sync group: 100 server endpoints
- Server endpoints per server: 30 server endpoints
- File system objects (directories and files) per sync group: 100 million objects
- Maximum number of file system objects (directories and files) in a directory: 5 million objects
- Maximum object (directories and files) security descriptor size: 64 KiB
- File size: 100 GiB
- Minimum file size for a file to be tiered: 64 KiB

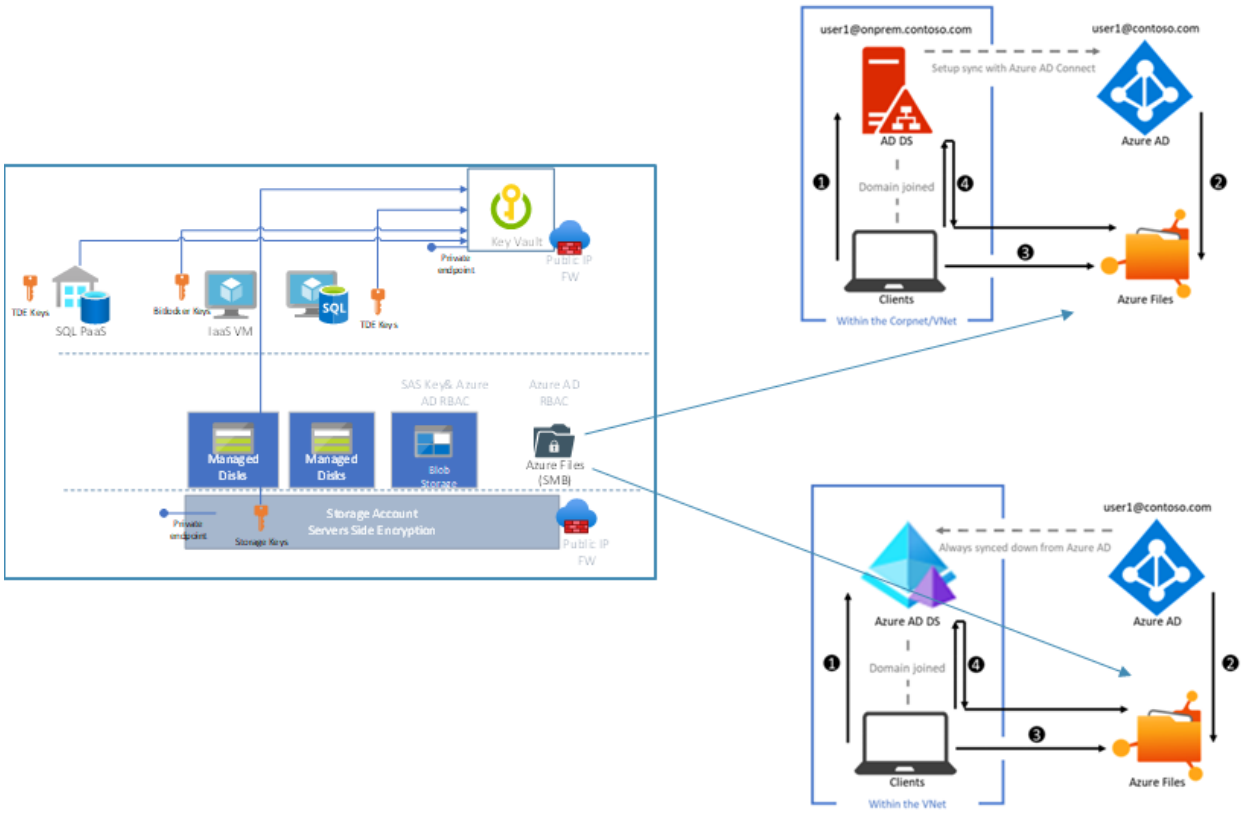
To access Azure Files resources with AD credentials, Service principle must have necessary permissions at the share level. This process is similar to specifying Windows share permissions, where you specify the type of access that a particular user has to a file share.

There are 3 built in RBAC roles for granting share-level permissions:

- Storage File Data SMB Share Reader allows read access in Azure Storage file shares over SMB
- Storage File Data SMB Share Contributor allows read, write, and delete access in Azure Storage file shares over SMB
- Storage File Data SMB Share Elevated Contributor allows read, write, delete and modify NTFS permissions in Azure Storage file shares over SMB

Recommendations

- Leverage Service Principle with necessary permissions and privileges to access Azure File shares



✓	**Recommendation - Azure AD Authentication Synced Access (SMB)** • Enable Azure files on-premises AD DS authentication, including creating an AD identity to present storage account • Assign Azure AD identity that was synced from AD on share level permission to Azure files. • Mount Azure Files with Storage account key and configure directory/file level permissions (Windows DACLs) to the AD identity • Access Azure Files using AD credentials by first authenticating against AD DS and sending the Kerberos token to Azure Files for authorization

In the bottom right portion of above picture Azure AD authentication only – difficult to maintain overtime – non-authoritative solution

- Enable Azure files on-premises AD DS authentication
- Assign Azure AD identity on share level permission to Azure files.
- Mount Azure Files with Storage account key and configure directory/file level permissions (Windows DACLs) to the AD identity
- Access Azure Files using AD credentials by first authenticating against Azure AD DS and sending the Kerberos token to Azure Files for authorization

9 Compute Security

Deploying application and security updates across client is probably a complex process that involves multiple stages. Image standardization, wherever OS, AKS, databases or applications allow to ensure consistency across deployments. These images typically include predefined security and configuration settings, and software workloads.

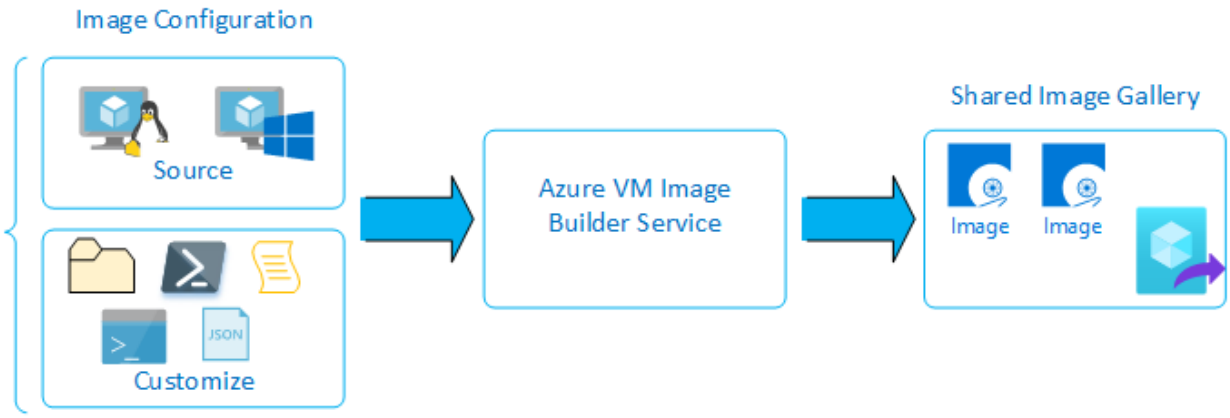
Client already have a build process of standardized images on-premise through their own imaging

pipeline or use the Azure VM Image Builder service. Using Azure VM Image Builder, you can quickly start building standardized images without needing to set up your own imaging pipeline. Just provide a simple configuration describing your image, submit it to the Image Builder service, and the image is built and distributed.

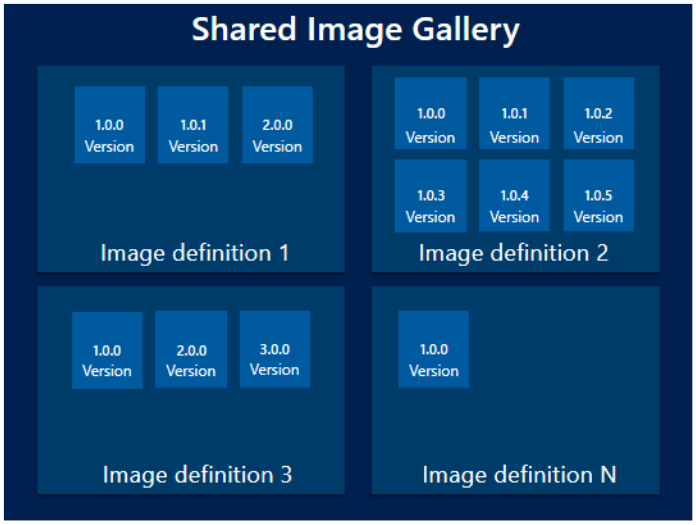
You can utilize Azure VM Image Builder with a Windows or Linux image from Azure Marketplace or your existing custom images and add your own customizations.

9.1.1 Azure Image Builder

Azure Image Builder is a custom image build process that creates standardized VM image to ensure consistent deployments in the cloud.



- Azure Shared Image Gallery (SIG) enables image distribution across multiple subscriptions and regions through a centralized image management platform.
- Shared Image Gallery (SIG) is a repository for sharing custom images and “umbrella” for Image definitions and versions
- Image Definition is a type of image (Windows/Linux) with RAM requirements, release notes.
- Image version is the version of the custom image stored under Image definition in SIG



With Azure Shared Image Gallery, you can:

- Move custom images to another region
- Deploy VMs from custom image in other subscription
- Create many instances from custom managed images without performance impact

9.1.2 VM security

Security in Azure is shared responsibility and we are responsible for how the infrastructure will be protected. Don't allow incidents to be initiators of tidying up security but better be proactive and always have in mind that you're responsible for the security of workloads in Azure. In order to provide highly available environments with 99.99% or higher SLAs, Microsoft group Virtual Machines in the Availability Sets or Availability Zones

Virtual Machines within an Availability Set run across multiple Microsoft physical servers, compute racks, storage and network devices. If a failure happens (whether it is hardware or software related, only certain VMs are impacted and your VM pool remaining Virtual Machines remain operational.

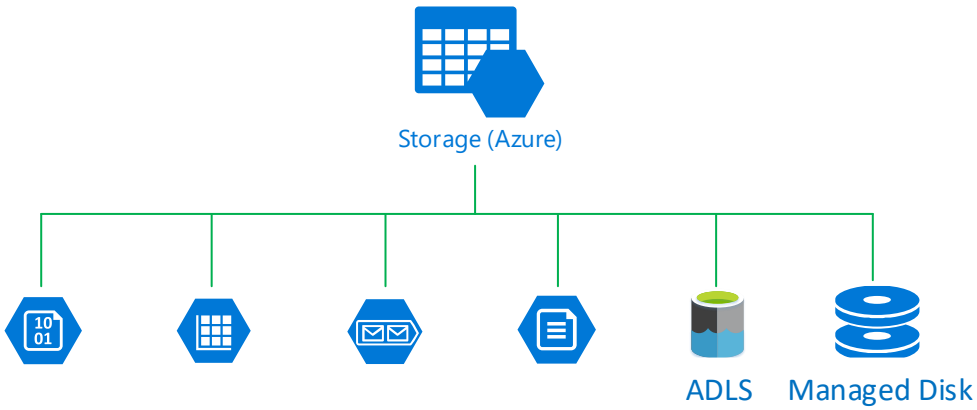
Availability Zone incorporates all the features from Availability Set but uses hardware racks from different Microsoft Data Centers within the same Azure region. It's a HA offering from Microsoft Azure that protects your applications and data from datacenter failures.

✓	**Recommendations** • Ensure approved extensions are installed and via Azure Policy • Ensure latest OS and Security patches on Windows images • Minimize the use of Public IPs • Leverage Azure Policy to enable Diagnostics Logs on VMs • Do not leave management ports open • VM Defender Advanced Threat protection • Windows Servers hardening on Windows images • Domain Join – managed domain services for Windows VMs • Always use least privilege approach – so you give users/developers exactly what they need

1.1. Managed Disks

Azure Managed Disks are block-level storage volumes configured with virtual machines and managed by Azure. When you select managed disk, you just need to specify the disk size, the disk type, and provision the disk. Once you provision the disk, Azure handles the rest.

Features	Managed Disks	Unmanaged Disks
Management	Is an ARM (Azure Resource Manager) object (resource)	Is a file (.vhd) residing on an Azure Storage Account.
Size	disks sizes are fixed (and can be resized). Which means that you cannot choose a custom size.	Can choose the disk size during the provisioning (and can be resized) when using Standard Storage.
Performance	Has a predictable performance, with standard HDD, with Standard SSD storage, Premium SSD storage, Ultra Disk offering	Only premium storage disks have a predictable performance. Standard storage has a predictable performance (500 IOPS) unless they are impacted by the Storage Account performance limits
Availability	When placing Azure VMs using managed disks under an Availability Set, disks are placed on different fault domains in order to achieve the better SLA	When placing Azure VMs using unmanaged disks under an Availability Set, there is no guarantee that disks are placed on different fault domains, even if they are on different Storage Accounts.
Redundancy	Locally Redundant Storage (LRS)	LRS, GRS (Geo-redundant storage)



✓	**Recommendations** • Ensure Virtual machines use managed disks. • Encrytion to be enabled on all the managed disks. • Audits when a virtual machine is created that does not use managed disks

10 Key Management

Key management is important for securing protected data in the architectural environment. A key management solution will effectively assist in the prevention of data breaches and allow to meet regulatory compliance standards.

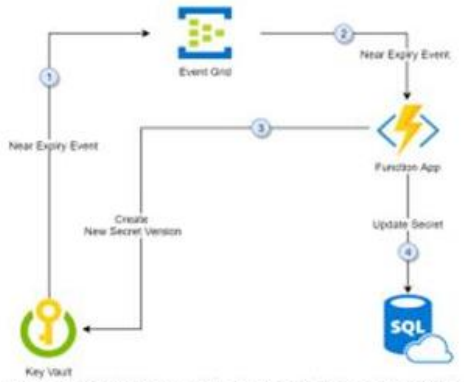
10.1.1 Azure Key Vault

Azure Key Vault is a key management cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, client need to secure access to key vaults by allowing only authorized applications and users. Azure Dedicated HSM is a cloud-based service that provides HSMs hosted in Azure datacenters that are directly connected to a customer's virtual network. These HSMs are dedicated network appliances (Gemalto's SafeNet Network HSM 7 Model A790) and only the customer has full administrative and cryptographic control over these devices

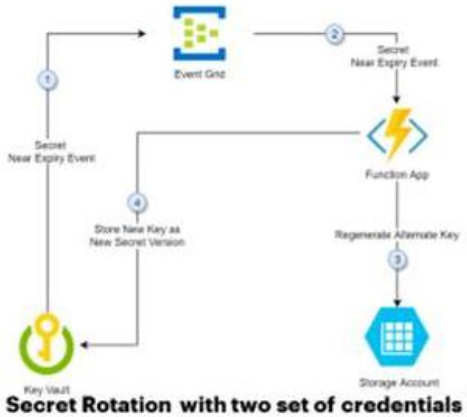
By default, Azure Key Vault has multiple layers of redundancy within the region where it is hosted, and it is replicated to another region within the same geographic region.

Secure Key Rotation by Key Vault - Key rotation on a regular basis helps meet industry standards and cryptographic best practices

- Azure Key Vault manages and rotates keys or passwords
- Automate the periodic rotation of secrets for databases and services that use one or two set of authentication credential stored in Azure Key Vault by using a function triggered by Azure Event Grid notification



Secret Rotation with one set of credentials



Secret Rotation with two set of credentials

✓	**Recommendation**: **Key Management** • Define and adopt a complete Key lifecycle Management process from creation to destruction • Use Azure Policy to enforce compliance and security standards for key vaults. • Use Azure AD for authentication and authorization of key vault access. • Use Azure Key Vault to manage and rotate encryption keys. • Use Azure Key Vault to manage and rotate application secrets. • Use Azure Key Vault to manage and rotate certificates. • Monitor key vault activity using Azure Monitor and Azure Log Analytics. • Use Azure Backup to back up key vault data. • Limit access to key vaults to only authorized users and applications. • Use Azure RBAC to manage access to key vaults.

11 Secure Logging & Monitoring

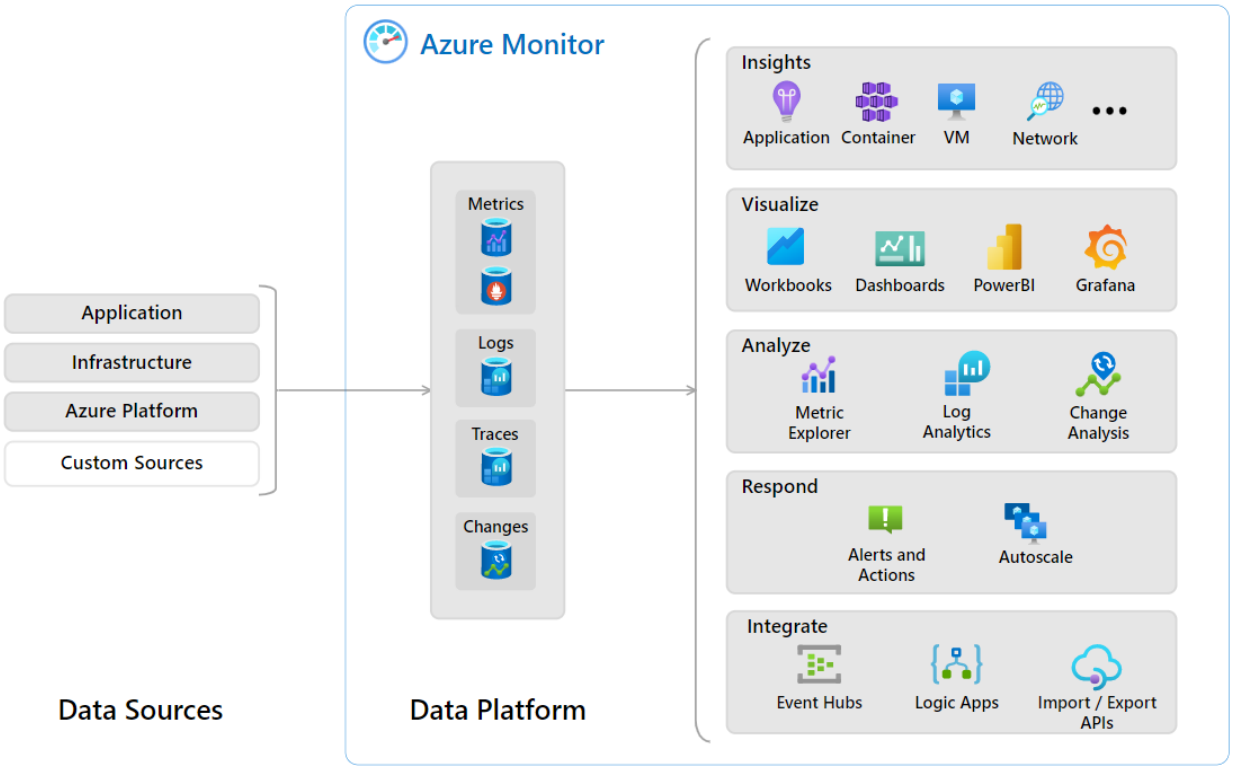
Secure logging and monitoring are integral components to maintain robust cybersecurity infrastructure. Effective monitoring relies on proportionate, reliable logging and device management practices.It helps to identify patterns of activity on networks, which in turn provide indicators of compromise.In the event of incidents, logging data can help to more effectively identity the source and the extent of compromise.

An effective log data collection and analysis process should incorporate tools to quickly and easily review audit logs for evidence of critical events.

11.1.1 Azure Monitor

Azure Monitor is a service offered by Azure to monitor and maximize the availability and performance of various resources. It delivers a comprehensive solution for collecting, analyzing data about how applications and services performing and proactively identify issues.

The following flow gives a high-level view of Azure Monitor.



Azure Monitor stores data as metrics, logs, disctibutes traces or changes. Azure Monitor aggregates and correlates data across multiple Azure subscriptions and tenants, in addition to hosting data for other services. Because this data is stored together, it can be correlated and analyzed using a common set of tools.

Azure Resource logs: Resource Logs provide information and insight into operations that were performed within an Azure resource (the data plane). Resource log content varies by the Azure resource

type. These logs are made visible by sending them to a destination that can be a Log Analytics workspace, Azure Storage account or Azure Event Hub, and this is setup in the Diagnostic Settings of that resource.

Azure Activity Log: There is a single log that provides insight into operations on each Azure resource in a subscription from the outside (the management plane). These are what, who and when of any write operation taken on the resources in a Subscription. Activity Log of a Subscription can be exported to a Log Analytics workspace, Azure Storage account or Azure Event Hub as setup in the Diagnostic Setting.

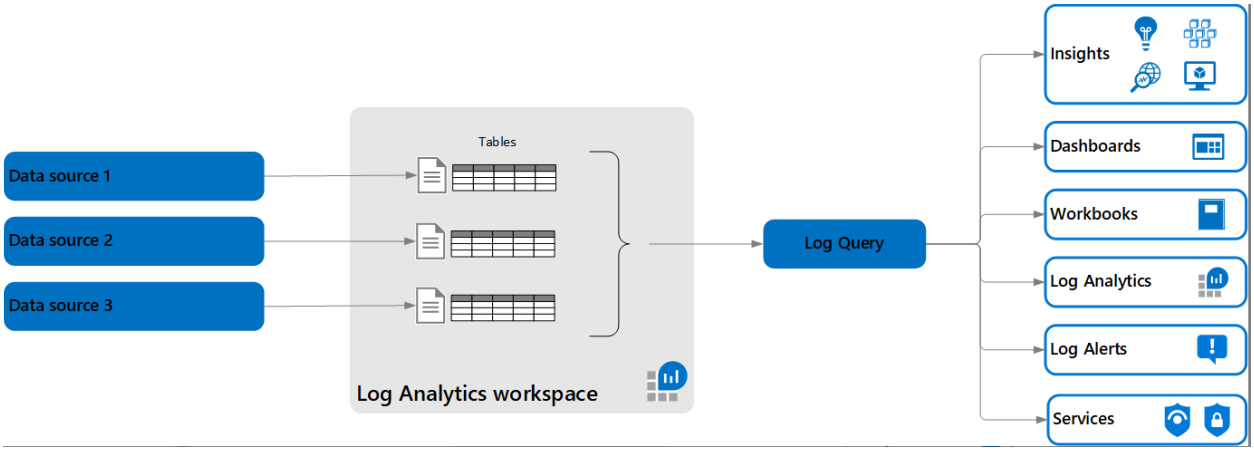
Azure Active Directory Logs: These logs contain the history of sign-in activity and audit trail of changes made in the Azure Active Directory for a tenant. This is a tenant level export and can be setup using Diagnostic setting of AAD and data collected will include data for all subscriptions in the AAD tenant.

11.1.2 Log Analytics Workspace

Azure Log Analytics Workspace is a logical storage unit in Azure where all log data generated by Azure Monitors are stored.Its a unique environment for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud.

Single workspace can store all data collection otherwise multiple workspaces can also be created.

Each workspace contains multiple tables that are organized into separate columns with multiple rows of data.Log queries define columns of data to retrieve ad provide output to different features of Azure Monitor and other services that use workspaces.



✓	**Recommendation**: **Secure Logging & Monitoring** • Ensure Microsoft Defender of Servers configured to collect the logs from VM • Ensure Microsoft Defender for Cloud configured to collect critical security events • Workspace permissions are granted based on Azure RBAC control. • Ensure local authentication is disabled for Log Analytics using Azure Policy • Ensure policy exists for Azure Monitor if a log profile is enabled for exporting activity logs.

12 Vulnerability Management

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting and remediating security vulnerabilities across endpoints, workloads and systems.Security team leverages vulnerability management tool to detect vulnerabilities and utilize different processes to patch or remediate them.

Vulnerability – Its defined by the International Organization for Standardization (ISO 27002) as "weakness of an asset or group of assets that can be exploited by one of more threats".

Threat – It's something that can exploit a vulnerability.

Risk – It's the damage that could be cause by the open vulnerability being exploited by a threat.

Vulnerability management recommendations focus on addressing issues related to continuously acquiring, assessing, and acting on new information in order to identify and remediate vulnerabilities as well as minimizing the window of opportunity for attackers.

Vulnerability management is a cyclical process and it follows a set number of stages and it repeats.

In order to create an effective, ongoing vulnerability-management process, solutions should include following:

Scanning – It includes network scanning and firwall logging.

Finding – It involves analysing the scan results to identify vulnerabilities as well as possible evidence of past or occurring breaches.

Checking – It incorporates an assessment of the vulnerabilities themselves to determine how they may be used by threat actors and what risk they entail.

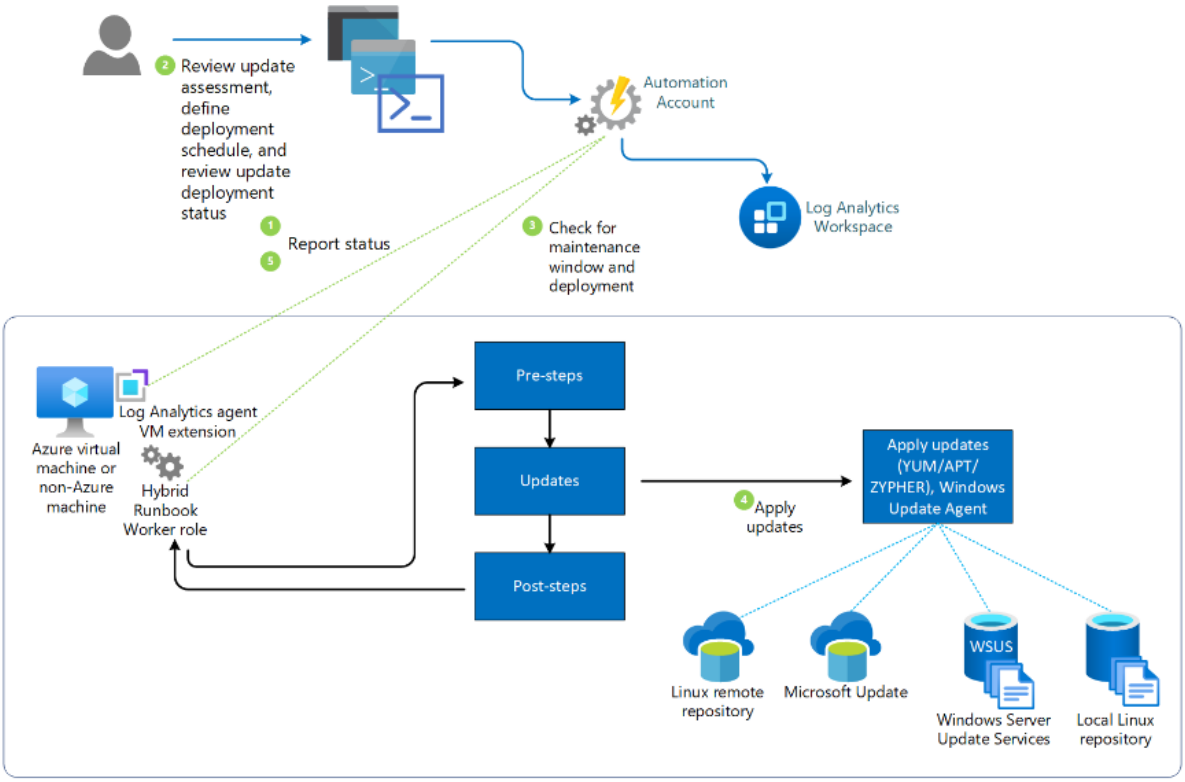
Patching – It involves patching identified vulnerabilities, effectively eliminating them as potential threat vectors.

Measuring – It involves assessing the effectiveness of the vulnerability-management solution

12.1.1 Patch/Update Management

Patch is a software update released to correct errors,bugs, or security vulnerabilities. Patch management is the critical practise in keeping systems updated, reducing attack surfaces.

Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines in Azure, physical or VMs in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management.



Deploy and install software updates on machines that require the updates by creating a scheduled deployment. Updates are installed by runbooks in Azure Automation. You can't view these runbooks, and they don't require any configuration. When an update deployment is created, it creates a schedule that starts a master update runbook at the specified time for the included machines.

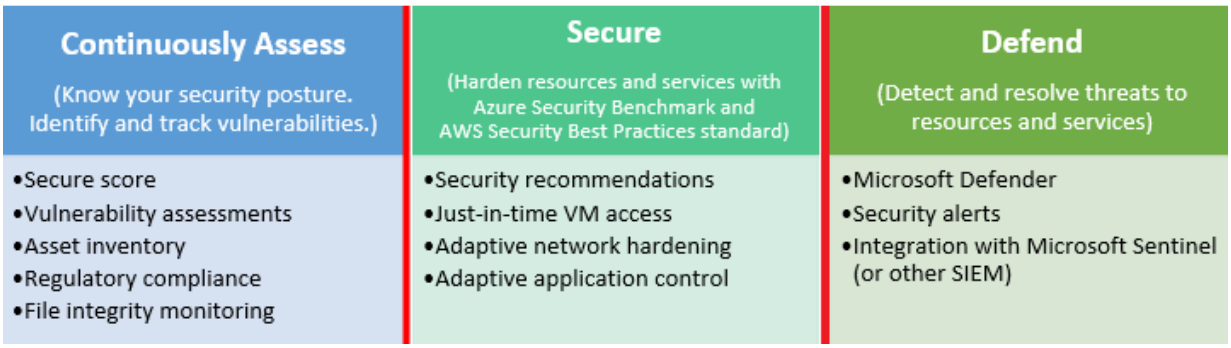
12.1.2 Defender for Cloud

Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform for all of your Azure, on-premises, and multicloud resources.

CSPM is to remediate security issues and improve security posture.

- Generates a secure score for your subscriptions based on an assessment of connected resources compared with Microsoft cloud security benchmark.
- Provides hardening recommendations based on any identified security misconfigurations and weaknesses.

CWP(Cloud Workload Protection Platform) is to identify unique workload security requirement, which facilitates security alerts powered by Microsoft Threat Intelligence via Defender for Cloud.



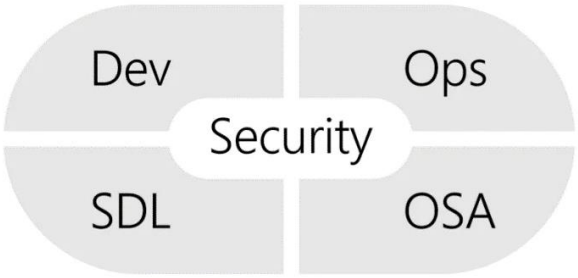
Defender for Cloud continuously discovers new resources that are being deployed across your workloads and assess whether they are configured according to security best practices. If not, they're flagged and you get notified with the prioritized list of recommendations what needs to fixed.

✓	**Recommendation**: Vulnerability Management • Ensure policies enabled to align your deployment with organizational standards. • Ensure new VM builds adhere with the organizational Security Baseline. • File integrity monitoring enabled using Defender for Cloud on VM's. • VM's should have Vulnerability assessment solution. • Create a baseline of approved updates that can be used to evaluate the compliance of your VMs and servers. • Use Azure Monitor to track the status of update deployments and to receive notifications about update failures.

✎	**Note:** • Update management solution not in current scope. • Existing solution (if in place) to be leveraged for patching the VM's.

13 Secure DevOps

Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity.



The practices used in DevOps provide a great opportunity to improve security. Practices such as automation, monitoring, collaboration, and fast and early feedback provide a great foundation to build security into DevOps processes

As new types of cybersecurity attacks rise, harden your development environment and software supply chain by integrating security early in the development cycle. DevSecOps combines GitHub and Azure products and services to foster collaboration between DevOps and SecOps teams

13.1.1 Azure DevOps

Azure DevOps is a software as a service platform from Microsoft.This service provides a toolchain that allows teams to develop and deploy software.It has integration with tools and services that allows flexibility and promotes collaboration.

Azure DevOps supports a collaborative culture and set of processes that bring together developers, project managers, and contributors to develop software. It allows organizations to create and improve products at a faster pace than they can with traditional software development approaches.

13.1.2 DevOps Boards

Azure Boards provides software development teams with the interactive and customizable tools they need to manage their software projects.It provides a rich set of capabilities including native support for Agile,Scrum, and Kanban processes, configurable dashboards and integrated reporting.

This helps to quickly and easily track work, issues, and code defects associated with migration.

Azure Boards provides several hubs, each providing a set of interactive tools. Use the **Boards** hub to view work items as cards and perform quick status updates through drag-and-drop. The feature is similar to sticky notes on a physical whiteboard. Use to implement Kanban practices and visualize the flow of work for a team.

13.1.3 Repos

Azure Repos is a set of version control tools that you can use to manage your code. Whether your software project is large or small, using version control as soon as possible is a good idea.

Version control systems are software that help you track changes you make in your code over time. As you edit your code, you tell the version control system to take a snapshot of your files. The version control system saves that snapshot permanently so you can recall it later if you need it. Use version control to save your work and coordinate code changes across your team.

Azure Repos provides two types of version control:

- Git: distributed version control
- Team Foundation Version Control (TFVC): centralized version control

Git is the most commonly used version control system today and is quickly becoming the standard for version control. Git is a distributed version control system, meaning that your local copy of code is a complete version control repository. These fully functional local repositories make it is easy to work offline or remotely. You commit your work locally, and then sync your copy of the repository with the copy on the server.

Azure Repos also supports Team Foundation Version Control (TFVC). TFVC is a centralized version control system. Typically, team members have only one version of each file on their dev machines. Historical data is maintained only on the server. Branches are path-based and created on the server.

13.1.4 Build and Release Pipelines

Azure Pipelines provides build and release services to support continuous integration and delivery of applications.

Azure Pipelines automatically builds and tests code projects. It supports all major languages and project types and combines continuous integration, continuous delivery, and continuous testing to build, test, and deliver your code to any destination.

Azure Pipelines provides a quick, easy, and safe way to automate building your projects with consistent and quality code that's readily available to users.

✓	**Recommendation**: Secure DevOps • Use AAD for authentication to ensure that only authorized users have access to Azure DevOps. • Use Azure Policy to enforce compliance with security standards and to ensure that Azure DevOps resources are configured securely. • Use Azure Key Vault to manage secrets, such as passwords and connection strings, used by Azure DevOps. • Use Azure RBAC to manage access to Azure DevOps resources, including repos, pipelines, and artifacts. • Use Azure DevOps extension security to ensure that only trusted extensions are installed and that they are running securely. • Use Multi-Factor Authentication (MFA) to increase security for Azure DevOps users and administrators. • Set Branch policies such that no code is committed to main/master branch irectly. And approvals to be set according to team structure.

	• Repo access to be controlled using inbuild policies to avoid any unauthorized access to the code. • Pipelines should have approvals before the deployment is kicked off.