AZURE SECURITY FOUNDATIONS BENCHMARK (DRAFT)

Azure security recommendations

September 30, 2019

Disclaimer

This document is for informational purposes only. MICROSOFT MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this white paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Executive Summary

The Azure Security Foundations Benchmark contains security recommendations, and information on how to implement them, that will help improve the security posture with respect to Azure resources within an organization. This document includes benchmark recommendations for Azure and shows how they apply to individual Azure services. This document is for anyone interested in Azure security and improving their overall security posture. This includes IT professionals in the areas of cloud development, infrastructure and operations, compliance, research, audit, and policy development.

Contents

Introduction

Your company may have several years or even decades of experience with on-premises computing. You know how to secure those deployments. But the cloud is different. How do you know if your cloud deployments are secure? What are the differences between on-premises security practices and those in the cloud?

There is a dizzying array of white papers, best practices, reference architectures, web guidance, open source tools, commercial solutions, intelligence feeds, and more that can be used to help secure the cloud. Which ones should you use? What can you do with the least amount of effort to get an acceptable level of security?

One of the best ways to get a leg up on securing your cloud deployments is to focus on the most impactful cloud security best practices. Best practices for securing any service begin with a fundamental understanding of cybersecurity risk and how to manage it. You can then leverage this understanding by using security recommendations from your service provider to help guide your risk-based decisions as they are applied to specific security configuration settings in your environment.

Azure Security Foundations Benchmark helps improve security

Azure recommends following a risk management framework such as the one described in NIST 800-37 rev 1. The Azure Security Foundations Benchmark contains recommendations that help you improve the security of your applications and data on Azure.

This benchmark contains recommendations that help you improve the security of your applications and data on Azure. The recommendations in this document will ultimately go into updating the CIS Microsoft Azure Foundations Benchmark v1, and are anchored on the security best practices defined by the CIS Controls®, Version 7.

In addition, these recommendations will be integrated into Azure Security Center and their impact will be surfaced in the Azure Security Center Secure Score and the Azure Security Center Compliance Dashboard.

The Azure Security Foundations Benchmark has recommendations for the following CIS security controls:

- Network
- Logging
- Monitoring
- Identity and access management
- Data protection

About this document

Our primary goal for the release of this document is to provide the security community an opportunity to contribute to the Azure Security Foundations benchmark.

The Azure Security Foundations Benchmark is in draft stage and we'd like to get your input. Specifically, we'd like to know:

- Does this document provide you the information needed to understand how to define your own security baseline for Azure based resources?
- Does this format work for you? Are there other formats that would make it easier for you to use the information and act on it?
- Do you currently use the CIS Controls as a framework and the current edition of the CIS Azure Security Foundations Benchmarks?
- What additional information do you need on how to implement the recommendations using Azure security related capabilities?
- Once we have the final version of the benchmark ready, we will be integrating with Azure Security Center Compliance Portal. Does this meet your requirements of monitoring Azure resources based on CIS Benchmarks™?

There are two ways you can let us know what you think and the answers to these questions:

- Send us an email
- Fill in the feedback form at https://aka.ms/AzSecBenchmark

This document clarifies terms, and then it lists the recommendations for each of the Security control categories. This is followed by information about how to implement these recommendations in the core Azure services. Consider the recommendations in this document as a starting point. You may build on these and extend them based upon corporate, industry, and governmental security and compliance requirements.

Security controls, benchmarks, and baselines

There's a process for figuring out what you need to do to ensure your application, data, or environment is secure. The process involves defining industry-wide standards or controls, service-provider benchmark recommendations, and then your own organizational security baseline requirements.

Term	Description	Example
Control	A **control** is a high-level description of a feature or activity that needs to be addressed. It is neither technology nor implementation specific.	For example, Data Protection is one of the CIS security controls. This control contains specific actions that need to be addressed to help ensure data is protected.
Benchmark	A **benchmark** contains security recommendations for a specific technology, such as Azure. The recommendations are based on controls.	For example, the Azure Security Cloud Benchmark is based on the security controls defined by the Center for Internet Security (CIS).
Baseline	A **baseline** is the security requirements for an organization. The security requirements are based on benchmark recommendations. Each organization decides which benchmark recommendations to implement.	For example, the Contoso company creates its security baseline by choosing to require specific recommendations in the Azure Security Cloud Benchmark.

For more information on controls, benchmarks, and baselines, see the Appendix.

Azure Security Foundations security recommendations

The Azure Security Foundations Benchmark contains recommendations for networking, logging, monitoring, identity and access management, and data protection. Each recommendation in the Azure Security Foundations Benchmark has the following information.

The security recommendation tables contain the following components:

- **Rec ID** – is the Azure Security Foundations ID that corresponds to this recommendation.
- **CIS sub-control ID** – is the CIS sub-control ID that corresponds to this recommendation.
- **Recommendation ID** – is a number assigned to each Azure Security Foundations Benchmark recommendation. Recommendation IDs help with tracking rules for auditing and compliance purposes. They can also be used in automated solutions to help track compliance and configuration drift.
- **Recommendation –** is the action or task for implementation. For example, Azure recommends, within the Network Security section, to "Ensure that only network ports, protocols and services listening on a system with validated business needs, are running on each service".
- **Implementation -** explains how to implement the recommendation on Azure, plus links to documentation for more information.
- **Responsibility -** explains whether the customer or the service-provider is responsible for implementing this recommendation. Security responsibilities are shared in the public cloud. Some security controls are only available to the cloud service provider and therefore responsibility for addressing those controls falls on Microsoft Azure.

Network recommendations

Network security recommendations focus on specifying which network protocols, TCP/UDP ports, and network connected services are allowed or denied access to Azure services.

The following table lists the recommendations for network security.

Rec ID	CIS ID	Recommendation	Implementation	Responsibility
1.1	9.1	Ensure access to resources is routed through the subscription's virtual network	We recommend customers always configure their Azure resources to use a virtual network within their subscription. For virtual machines this is the default. For dedicated managed resources this is via configuration of the networking options of the resource.	Customer using available Azure networking features

			For shared resources use either the private link or legacy service endpoint option. Virtual Network Service Endpoints Network Security Groups See the Network security capability section to learn about how to use these features for various core Azure Services.	
1.2	9.2	Ensure that only network ports, protocols and services listening on a system with validated business needs, are running on each service.	We recommend that customers ensure all subnet's and NICs are associated with an NSG, or in the case of classic resources to ACLs, which limit the allowed Destination Ports, Destination IPs and Source IPs to those that are required for your business needs. In addition, we recommend that customers use ASC JIT network access to restrict access to management ports to only the length of time and remote sources necessary at any given point in time. Network Security Groups Azure Firewall Azure Security Center JIT See the Network security capability section to learn about how to use these features for various core Azure Services.	Customer using available Azure networking features
1.3	9.3	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	We recommend that customers enable Network Watcher and use ASC Network Recommendations to monitor NSG Configuration and Traffic.	Customer using available Azure network security features
1.4	9.4	Apply host-based firewalls or port filtering tools on end systems,	Customers may optionally use native OS firewall configuration on VM's to provide additional	Customer using available Azure

		with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	application specific, authenticated or IP filtering.	network security features

Table 1 Network recommendations

Logging recommendations

Security logging recommendations focus on activities related to enabling, acquiring, and storing audit logs for Azure services.

The following table lists the recommendations for security logging.

Rec ID	CIS ID	Recommendation	Implementation	Responsibility
2.1	6.2	Activate audit logging: Ensure that local logging has been enabled on all systems and networking devices.	Ensure auditing and logging features are enabled on Azure resources. Azure logging and auditing Overview of Azure Diagnostic Logs Refer to the Security logging capability section and Security Monitoring capability section to learn about how to use these features for various core Azure services.	Customer onboard to Azure Monitor and Azure Security Center to receive different logs that is available for their environment.
2.2	6.3	Enable Detailed Logging: Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	Enable Azure Monitor and logging capability. Overview of Azure Diagnostic Logs Refer to the Security logging capability section to learn about how to use these features for various core Azure services.	Customer onboard to Azure monitor and enable logging
2.3	6.4	Ensure adequate storage for logs: Ensure that all systems that store logs have adequate storage space for the logs generated.	Provision Azure storage for log storage. Introduction to Azure Storage	Customer provision storage for storing their logs.

2.4	8.8	Enable Command-line Audit Logging: Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	Azure Security Center has detections on malicious process execution. Azure Security Center detection capabilities Refer to the Security Monitoring capability section to learn about how to use these features for various core Azure services.	Customer to use Azure Security Center.

Table 2 Logging recommendations

Monitoring recommendations

Recommendations focus on analyzing logs with the goal of generating alerts for possible security events.

The following table lists the recommendations for security monitoring.

Rec ID	CIS ID	Recommendation	Implementation	Responsibility
3.1	4.8	Log and alert on changes to administrative group membership: Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	What is Azure Active Directory Identity Protection?	Customer onboard to Azure AD premium.
3.2	4.9	Log and alert on unsuccessful administrative account login: Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Quickstart: Onboard your Azure subscription to Security Center Standard Refer to the Security Monitoring capability section to learn about how to use these features.	Customer onboard to Azure Security Center.
3.3	6.5	Central log management: Ensure that appropriate logs are being aggregated to a central log	Enable Azure Security Center or Azure Sentinel to analyze the logs and build detections. Quickstart: Onboard your Azure subscription to Security	Customer onboard to Azure Security Center or Azure Sentinel.

		management system for analysis and review.	Center Standard Onboard Azure Sentinel Refer to the Security Monitoring capability section to learn about how to use these features.	
3.4	6.6	Deploy SIEM or log analytic tool: Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	Azure Monitor Azure Sentinel Documentation	Customer enable Azure Monitor and Azure Sentinel.
3.5	6.7	Regularly review logs: On a regular basis, review logs to identify anomalies or abnormal events.	Regularly review your logs on Azure Monitor.	Customer review their logs and activities on what is happening in their environment.
3.6	8.6	Centralize anti-malware logging: Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	Antimalware logs are collected in Azure Security Center. Quickstart: Onboard your Azure subscription to Security Center Standard Refer to the Security Monitoring capability section to learn about how to use these features.	Customer onboard to Azure Security Center
3.7	16.13	Alert on account login behavior deviation: Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Azure AD protection provides detections for unusual user activities. What is Azure Active Directory Identity Protection?	Customer onboard to Azure AD premium.

Table 3 Monitoring recommendations

Identity and access management recommendations

Identity and access management recommendations focus on addressing issues related to identity-based access control, locking down administrative access, alerting on identity-related events, abnormal account behavior, and role-based access control.

The following table lists the recommendations for identity and access management.

Rec ID	CIS ID	Recommendation	Implementation	Responsibility
4.1	4.1	Maintain inventory of administrative accounts: Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	For ARM, customers can use the user access blade to monitor for ARM RBAC assignments. Also, Azure PIM to prevent persistent ARM subscription access. View activity and audit history for Azure resource roles in PIM Refer to the Identity and Access Management capability section to learn about how to use these features for various core Azure services.	Customer for IaaS Customer for ARM
4.2	4.5	Use multifactor authentication for all administrative access: Use multi-factor authentication and encrypted channels for all administrative account access.	AAD MFA for services with data plane AAD RBAC. How it works: Azure Multi-Factor Authentication Refer the Identity and Access Management capability section to learn about how to use these features for various core Azure Services.	Customer for setting up MFA.
4.3	4.7	Limit access to script tools: Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	ARM RBAC allows teams to scope privilege to least access required. Reader role or data reader role for non-developers. Refer to the Identity and Access Management capability section to learn about how to use these features for various core Azure Services	Customer for setting up RBAC.

4.4	4.8	Log and alert on changes to administrative group membership: Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	Azure Monitor + Activity logs to track RBAC changes. Diagnostic logs to track Data Plane RBAC changes. View activity logs for RBAC changes to Azure resources	Customer for using AAD audit logs and establishing monitors.
4.5	4.9	Log and alert on unsuccessful administrative account Login: Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Azure AAD audit logs can track this. Audit activity reports in the Azure Active Directory portal. Pair it with Sentinel or 3rd party SEIM.	Customer for using AAD audit logs and establishing monitors.
4.6	13.4	Only allow access to authorized cloud storage or email providers: Only allow access to authorized cloud storage or email providers.	Storage now supports ARM RBAC for AAD. It can also be placed into vNet. Authenticate access to Azure blobs and queues using Azure Active Directory	Customer to use RBAC instead of SAS keys.
4.7	14.6	Protect information through access control lists: Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	Data Plane AAD Support for Storage Accounts Authenticate access to Azure blobs and queues using Azure Active Directory	Customer to use RBAC instead of SAS keys.

4.8	16.13	Alert on account login behavior deviation: Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Azure Activity Directory Identity Protection. What is Azure Active Directory Identity Protection?	Customer to setup AAD Identity protection.

Table 4: Identity and access management recommendations

Data protection recommendations

Data protection recommendations focus on addressing issues related to encryption, access control lists, identity-based access control, and audit logging for data access.

The following table lists the Azure security recommendations for data protection.

Rec ID	CIS ID	Recommendation	Implementation	Responsibility
5.1	14.8	Encrypt sensitive information at rest: Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, to access the information.	Azure encryption provides a variety of models for encryption at rest. Azure encryption overview Refer the Data Protection capability section to learn about how to use these	Customer to use Azure encryption services. features for various core Azure Services.
5.2	13.4	Only allow access to authorized cloud storage or email providers: Only allow access to authorized cloud storage or email providers.	Storage now supports ARM RBAC for AAD. It can also be placed into vNet. Authenticate access to Azure blobs and queues using Azure Active Directory	Customer to use RBAC instead of SAS keys.
5.3	14.6	Protect Information through access control lists: Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only	Data Plane AAD Support for Storage Accounts. Authenticate access to Azure blobs and queues using Azure Active Directory)	Customer to use RBAC instead of SAS keys.

		authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.		
5.4	14.9	Enforce detail logging for access or changes to sensitive data: Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	Depends upon where the data is stored (VM, database, Azure Storage, etc.) - Azure logging and auditing provide tools. Azure logging and auditing	Customer to use Azure logging and auditing

Table 5 Data protection recommendations

Security implementations in Azure services

This section shows how the Azure security recommendations discussed in the previous sections are implemented in core Azure services. The implementations include links to the documentation to help you understand how to apply each aspect of security to your situation.

The implementations listed do not necessarily fulfill all Azure security recommendations. The tables are a tightly scoped collection of security capabilities for each service. Future versions of this document will include an expanded set of capabilities.

The service implementation tables contain the following components:

- **Service** – is the service being mapped to security capabilities
- **Implementation** – is what Azure security capability is being mapped
- **Status** – is the current state of the security capability being mapped. Status is denoted as:
    - **Available** – is currently available
    - **In progress** – work has started
    - **Roadmap** – currently in the planning stage
    - **NA** – Not applicable to the service
- **Documentation** – provides a link to the security capability or current state of documentation for the security capability

Network implementations

The network security implementation table maps core Azure security services to one of three Azure network security capabilities that can help you fulfill recommendations defined in this Azure Security Benchmark documentation.

Azure security capabilities included in the mapping include:

- **vNet connection** – ability to deploy service resources in your own virtual network
- **Service endpoints** – extends an Azure virtual network identity and address space to Azure PaaS services
- **NA** – not applicable

Service	Implementation	Implementation Status	Documentation Status
COMPUTE			
API Management	vNet connection	**Available**	How to use API Management with Azure Virtual Networks
App Service	vNet connection	**Available**	Security recommendations for App Service
Batch	vNet connection	**Available**	Create an Azure Batch pool in a virtual network
Cloud Services (Classic)	vNet connection (classic)	**Available**	Roadmap
Linux Virtual Machines	vNet connection	**Available**	Secure Linux network traffic
Mobile Apps	vNet connection	**Roadmap**	Roadmap
Service Fabric	vNet connection	**Available**	NSG configuration for Service Fabric clusters (Applied at VNET level)
Virtual Machine Scale Sets	vNet connection	**Available**	Virtual Machine Scale Sets FAQ
Web Apps	vNet connection	**Available**	Security recommendations for App Service
Windows Virtual Machines	vNet connection	**Available**	Secure network traffic
ANALYTICS			
Azure Data Lake Storage	Service endpoints	**Available**	Virtual network integration
Azure Databricks	vNet connection	**Available**	Quickstart: Create an Azure Databricks workspace in a Virtual Network
Azure Stream Analytics	NA	**NA**	NA

Data Lake Analytics	NA	**NA**	Roadmap
Event Hubs	Service endpoints	**Available**	Add virtual network service endpoint
HDInsight	vNet connection	**Available**	Extend Azure HDInsight using an Azure Virtual Network
Power BI Embedded	NA	**NA**	NA
CONTAINERS			
Azure Kubernetes Service	vNet connection	**Available**	Configure Azure CNI networking in Azure Kubernetes Service (AKS)
Azure Functions	vNet connection	**Available**	Tutorial: integrate Functions with an Azure Virtual Network
Container Instances	vNet connection	**Available**	Deploy container instances into an Azure virtual network
Container Registry	vNet connection Service endpoints	**Available**	Restrict access to an Azure container registry using an Azure virtual network or firewall rules
DATABASES			
Azure Cache for Redis	Service endpoints	**Roadmap**	Roadmap
Azure Cosmos DB	Service endpoints	**Available**	FAQ: Access Azure Cosmos DB from virtual networks
Azure Data Explorer (Kusto)	Service endpoints	**Roadmap**	Roadmap
Azure Database for MySQL	Service endpoints	**Available**	Use Virtual Network service endpoints and rules for Azure Database for MySQL
Azure Database for PostgreSQL	Service endpoints	**Available**	Use Virtual Network service endpoints and rules for Azure Database for PostgreSQL - Single Server
Azure SQL Database	Service endpoints	**Available**	Use virtual network service endpoints and rules for database servers
Azure Data Factory	Service endpoints	**Roadmap**	Data movement security considerations

SQL Data Warehouse	Service endpoints	**Available**	Use virtual network service endpoints and rules for database servers
STORAGE			
Azure Backup	Service endpoints	**Roadmap**	Roadmap
Azure Blob Storage	Service endpoints	**Available**	Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
File Storage	Service endpoints	**Available**	Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
Table Storage	Service endpoints	**Available**	Roadmap
Storage Accounts	Service endpoints	**Available**	Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
SECURITY			
Azure Key Vault	Service endpoints	**Available**	Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal

Table 4 Network security service implementations

Logging and Monitoring implementations

The security logging and monitoring implementation table maps core Azure security services to the Azure Monitor logging and monitoring capabilities that can help you fulfill recommendations defined in this document.

Azure security logging capabilities include:

- **Azure Monitor logs** – ability to log events to the Azure Monitor logs
- **NA** – not applicable

Service	Implementation	Implementation Status	Documentation
COMPUTE			
API Management	Azure Monitor logs	Available	Monitor activity logs
App Service	Azure Monitor logs	Roadmap	
Batch	Azure Monitor logs	Available	Batch metrics, alerts, and logs for diagnostic evaluation and monitoring
Cloud Services (Classic)	Azure Monitor logs	Available	Introduction to Cloud Service Monitoring
Linux Virtual Machines	Azure Monitor logs	Available	How to monitor Virtual Machines in Azure
Mobile Apps	Azure Monitor logs	Roadmap	Roadmap
Service Fabric	Azure Monitor logs	Roadmap	
Virtual Machine Scale Sets	Azure Monitor logs	Available	Virtual Machine scale sets FAQ
Web Apps	Azure Monitor logs	Roadmap	Enable diagnostics logging for apps in Azure App Service
Windows Virtual Machines	Azure Monitor logs	Available	How to monitor Virtual Machines in Azure
ANALYTICS			
Azure Data Lake Storage	Azure Monitor logs	Roadmap	Roadmap
Azure Databricks	Azure Monitor logs	Available	Roadmap
Azure Stream Analytics	Azure Monitor logs	Available	Troubleshoot Azure Stream Analytics by using diagnostics logs
Data Lake Analytics	Azure Monitor logs	Available	Accessing diagnostic logs for Azure Data Lake Analytics
Event Hubs	Azure Monitor logs	Available	Azure Event Hubs metrics in Azure Monitor
HDInsight	Azure Monitor logs	Available	Manage logs for an HDInsight cluster
Power BI Embedded	Azure Monitor logs	Available	Diagnostic logging for Power BI Embedded in Azure
CONTAINERS			

Azure Kubernetes Service	Azure Monitor logs	Available	Enable and review Kubernetes master node logs in Azure Kubernetes Service (AKS)
Azure Functions	Azure Monitor logs	Available	In planning
Container Instances	Azure Monitor logs	Available	Retrieve container logs and events in Azure Container Instances
Container Registry	Azure Monitor logs	Available	Roadmap
DATABASES			
Azure Cache for Redis	Azure Monitor Logs	Available	How to monitor Azure Cache for Redis
Azure Cosmos DB	Azure Monitor logs	Available	Diagnostic logging in Azure Cosmos DB
Azure Data Explorer (Kusto)	Roadmap	Roadmap	Roadmap
Azure Database for MySQL	Azure Monitor logs	Available	Monitoring in Azure Database for MySQL
Azure Database for PostgreSQL	Azure Monitor logs	Available	Monitor and tune Azure Database for PostgreSQL - Single Server
Azure SQL Database	Azure Monitor logs	Available	Monitoring and performance tuning
Azure Data Factory	Azure Monitor logs	Available	Alert and Monitor data factories using Azure Monitor
SQL Data Warehouse	Azure Monitor logs	Available	Monitor workload - Azure portal
STORAGE			
Azure Backup	Azure Monitor logs	Available	
Azure Blob Storage	Azure Monitor logs	Roadmap	Monitor a storage account in the Azure portal
File Storage	Azure Monitor logs	Roadmap	Enabling Storage Logging and Accessing Log Data
Table Storage	Azure Monitor logs	Roadmap	
Storage Accounts	Azure Monitor logs	Roadmap	Monitor a storage account in the Azure portal
SECURITY			

Azure Key Vault	Azure Monitor logs	Available	Azure Key Vault logging

Table 5 Security logging service implementations

Identity and access management implementations

The identity and access management implementations table maps core Azure security services to the Azure Active Directory authentication and Azure Active Directory multi-factor authentication security capabilities that can help you fulfill some of the recommendations defined in this Azure Security Benchmark document.

Identity and access management capabilities include:

- **AAD auth and MFA** – ability to use Azure Active Directory and multi-factor authentication
- **NA** – not applicable

Service	Implementation	Implementation Status	Documentation
COMPUTE			
API Management	AAD auth and MFA	Available	API Management features availability
App Service	AAD auth and MFA	Available	Tutorial: Authenticate and authorize users end-to-end in Azure App Service
Batch	AAD auth and MFA	Available	Authenticate Batch service solutions with Azure Active Directory
Cloud Services (Classic)	NA	NA	NA
Linux Virtual Machines	AAD auth and MFA	Available	https://docs.microsoft.com/azure/virtual-machines/linux/login-using-aad
Mobile Apps	AAD auth and MFA	Available	https://docs.microsoft.com/azure/app-service/configure-authentication-provider-aad?toc=%2fazure%2fapp-service-mobile%2ftoc.json
Service Fabric	AAD auth and MFA	Available	https://docs.microsoft.com/azure/service-fabric/service-fabric-cluster-creation-setup-aad

Virtual Machine Scale Sets	AAD auth and MFA	Available	Roadmap
Web Apps	AAD auth and MFA	Available	Tutorial: Authenticate and authorize users end-to-end in Azure App Service
Windows Virtual Machines	AAD auth and MFA	Roadmap	Roadmap
ANALYTICS			
Azure Data Lake Storage	AAD auth and MFA	Available	Access control in Azure Data Lake Storage Gen2
Azure Databricks	AAD auth and MFA	Available	Roadmap
Azure Stream Analytics	AAD auth and MFA	Roadmap	Roadmap
Data Lake Analytics	AAD auth and MFA	Available	Roadmap
Event Hubs	AAD auth and MFA	Available	Managed identities for Azure resources with Event Hubs
HDInsight	AAD auth and MFA	Available	Roadmap
Power BI Embedded	AAD auth and MFA	Available	Get an Azure AD access token for your Power BI application Register an Azure AD application to use with Power BI Create an Azure Active Directory tenant to use with Power BI
CONTAINERS			
Azure Kubernetes Service	AAD auth and MFA	Available	Access and identity options for Azure Kubernetes Service (AKS)
Azure Functions	AAD auth and MFA	Available	How to use managed identities for App Service and Azure Functions
Container Instances	AAD auth and MFA	Available	Security considerations for Azure Container Instances
Container Registry	AAD auth and MFA	Available	Authenticate with a private Docker container registry
DATABASES			

Azure Cache for Redis	AAD auth and MFA	Roadmap	Roadmap
Azure Cosmos DB	AAD auth and MFA	Roadmap	Roadmap
Azure Data Explorer (Kusto)	AAD auth and MFA	Available	Roadmap
Azure Database for MySQL	AAD auth and MFA	Roadmap	Roadmap
Azure Database for PostgreSQL	AAD auth and MFA	Roadmap	Roadmap
Azure SQL Database	AAD auth and MFA	Available	Use Azure Active Directory Authentication for authentication with SQL
Azure Data Factory	AAD auth and MFA	Available	Managed identity for Data Factory
SQL Data Warehouse	AAD auth and MFA	Available	Roadmap
STORAGE			
Azure Backup	AAD auth and MFA	Available	Use Role-Based Access Control to manage Azure Backup recovery points
Azure Blob Storage	AAD auth and MFA	Available	Authenticate access to Azure blobs and queues using Azure Active Directory
File Storage	AAD auth and MFA	Available	Overview of Azure Active Directory authentication over SMB for Azure Files (preview)
Table Storage	AAD auth and MFA	Available	In progress
Storage Accounts	AAD auth and MFA	Available	Authenticate access to Azure blobs and queues using Azure Active Directory
SECURITY			
Azure Key Vault	AAD auth and MFA	Available	Secure access to a key vault

Table 6 Identity and access management service implementations

Data protection implementations

The data protection service implementations table maps core Azure security services to capabilities for managing keys that can help you fulfill some of the recommendations defined in this Azure Security Benchmark document.

Data protection capabilities include:

- **Uses Azure Storage, which is encrypted** – service benefits from using encrypted Azure Storage
- **MSFT managed** – Microsoft manages the keys
- **Customer managed** – the customer manages the keys
- **NA** – not applicable

Service	Implementation	Status	Documentation
COMPUTE			
API Management	NA	NA	NA
App Service	NA (Has local cache but no persistent storage)	N/A	Azure App Service Local Cache overview
Batch	NA	NA	NA
Cloud Services (Classic)	NA	NA	NA
Linux Virtual Machines	MSFT managed Customer managed	Available	How to encrypt a Linux virtual machine in Azure
Mobile Apps	NA (Has local cache but no persistent storage)	NA	Azure App Service Local Cache overview
Service Fabric	NA	NA	NA
Virtual Machine Scale Sets	MSFT managed Customer managed	Available	Use Azure Disk Encryption with virtual machine scale set extension sequencing
Web Apps	NA (Has local cache but no persistent storage)	NA	Azure App Service Local Cache overview
Windows Virtual Machines	MSFT managed Customer managed	Available	Encrypt virtual disks on a Windows VM
ANALYTICS			
Azure Data Lake Storage	MSFT managed Customer managed	Available	Encryption of data in Azure Data Lake Storage Gen1
Azure Databricks	NA	NA	NA
Azure Stream Analytics	NA	NA	NA
Data Lake Analytics	NA	NA	NA
Event Hubs	MSFT managed	Roadmap	Roadmap

HDInsight	MSFT managed Customer managed	Roadmap	Available
Power BI Embedded	MSFT managed	Roadmap	Roadmap
CONTAINERS			
Azure Kubernetes Service	MSFT managed	Available	Security concepts for applications and clusters in Azure Kubernetes Service (AKS) – node security
Azure Functions	NA	NA	NA
Container Instances	MSFT managed	Available	Roadmap
Container Registry	MSFT managed	Available	Container image storage in Azure Container Registry
DATABASES			
Azure Cache for Redis	NA	NA	NA
Azure Cosmos DB	MSFT managed	Available	Data encryption in Azure Cosmos DB
Azure Data Explorer (Kusto)	MSFT managed	Available	Roadmap
Azure Database for MySQL	MSFT managed	Available	What is Azure Database for MySQL? – secure your data
Azure Database for PostgreSQL	MSFT managed	Available	What is Azure Database for PostgreSQL? – data security
Azure SQL Database	MSFT managed Customer managed	Available	Transparent data encryption for SQL Database and Data Warehouse
Azure Data Factory	MSFT managed	Available	Security considerations for data movement in Azure Data Factory
SQL Data Warehouse	MSFT managed Customer managed	Available	Transparent data encryption for SQL Database and Data Warehouse
STORAGE			
Azure Backup	MSFT managed	Available	Backup and restore encrypted Azure VM
Azure Blob Storage	MSFT managed Customer managed	Available	Azure Storage encryption for data at rest
File Storage	MSFT managed Customer managed	Available	Azure Storage encryption for data at rest

Table Storage	MSFT managed	Available	Azure Storage encryption for data at rest
Storage Accounts	MSFT managed Customer managed	Available	Azure Storage encryption for data at rest
SECURITY			
Azure Key Vault	Key Vault is an encryption technology	Available	What is Azure Key Vault?

Table 7 Data protection service implementations

Summary

Consider the recommendations in this document as a starting point. You may build on these and extend them, based upon corporate, industry, and governmental security and compliance requirements.

Service	vNet Integration Implementation Status	Azure Monitor Implementation Status	AAD auth and MFA Implementation Status	Data Protection Implementation Status
COMPUTE				
API Management	Available	Available	Available	NA
App Service	Available	Roadmap	Available	NA
Batch	Available	Available	Available	NA
Cloud Services (Classic)	Available	Available	NA	NA
Linux Virtual Machines	Available	Available	Available	Available
Mobile Apps	Roadmap	Roadmap	Available	NA
Service Fabric	Available	Roadmap	Available	NA
Virtual Machine Scale Sets	Available	Available	Available	Available
Web Apps	Available	Roadmap	Available	NA
Windows Virtual Machines	Available	Available	Roadmap	Available
ANALYTICS				
Azure Data Lake Storage	Available	Roadmap	Available	Available
Azure Databricks	Available	Available	Available	NA
Azure Stream Analytics	NA	Available	Roadmap	NA
Data Lake Analytics	NA	Available	Available	NA
Event Hubs	Available	Available	Available	Roadmap
HDInsight	Available	Available	Available	Available
Power BI Embedded	NA	Available	Available	Roadmap
CONTAINERS				

Azure Kubernetes Service	Available	Available	Available	Available
Azure Functions	Available	Available	Available	NA
Container Instances	Available	Available	Available	Available
Container Registry	Available	Available	Available	Available
DATABASES				
Azure Cache for Redis	Roadmap	Available	Roadmap	NA
Azure Cosmos DB	Available	Available	Roadmap	Available
Azure Data Explorer (Kusto)	Roadmap	Roadmap	Available	Available
Azure Database for MySQL	Available	Available	Roadmap	Available
Azure Database for PostgreSQL	Available	Available	Roadmap	Available
Azure SQL Database	Available	Available	Available	Available
Azure Data Factory	Roadmap	Available	Available	Available
SQL Data Warehouse	Available	Available	Available	Available
STORAGE				
Azure Backup	Roadmap	Available	Available	Available
Azure Blob Storage	Available	Roadmap	Available	Available
File Storage	Available	Roadmap	Available	Available
Table Storage	Available	Roadmap	Available	Available
Storage Accounts	Available	Roadmap	Available	Available
SECURITY				
Azure Key Vault	Available	Available	Available	Available

Appendix

More information about controls, benchmarks, and baselines

Security controls

CIS Security Controls, Version 7 is a prioritized set of security controls, developed by a community of IT experts, that identify areas of concern for security operations. The CIS controls are informed by actual attacks and reflect the combined knowledge of experts from every part of the ecosystem. Each control category has a list of sub-controls that more specifically identify areas to address. CIS Controls are not specific to a technology. Rather, they are intended to provide guidance for developing industry-wide benchmark recommendations for specific technologies. The benchmarks then guide organizations in the development of specific baseline requirements for their business, security and compliance needs.

Security benchmarks

Benchmarks are useful because they let you know what industry standards are for security in the cloud. Companies know what "good" security looks like on-premises but might not understand how what they do on-premises is done in the cloud. In addition, a benchmark might provide information on new settings and configurations as products evolve. Finally, these benchmarks help you compare the cloud service providers controls with those used in the enterprise.

Security baselines

Using cloud resources changes traditional risk calculations substantially. For this reason, a cloud-centric benchmark is a valuable tool to help you identify areas to evaluate when securing your cloud resources. The result of such evaluations defines a baseline that sets requirements within your organization for security configuration settings.