Security best practices for Azure solutions

April 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.

© 2018 Microsoft. All rights reserved.

Executive summary

This paper is a collection of security best practices to use when you’re designing, deploying, and managing your cloud solutions by using Microsoft Azure. These best practices come from our experience with Azure security and the experiences of customers like you.

This paper is intended to be a resource for IT pros. This might include designers, architects, developers, and testers who build and deploy secure Azure solutions.

For each best practice, our goal is to describe:

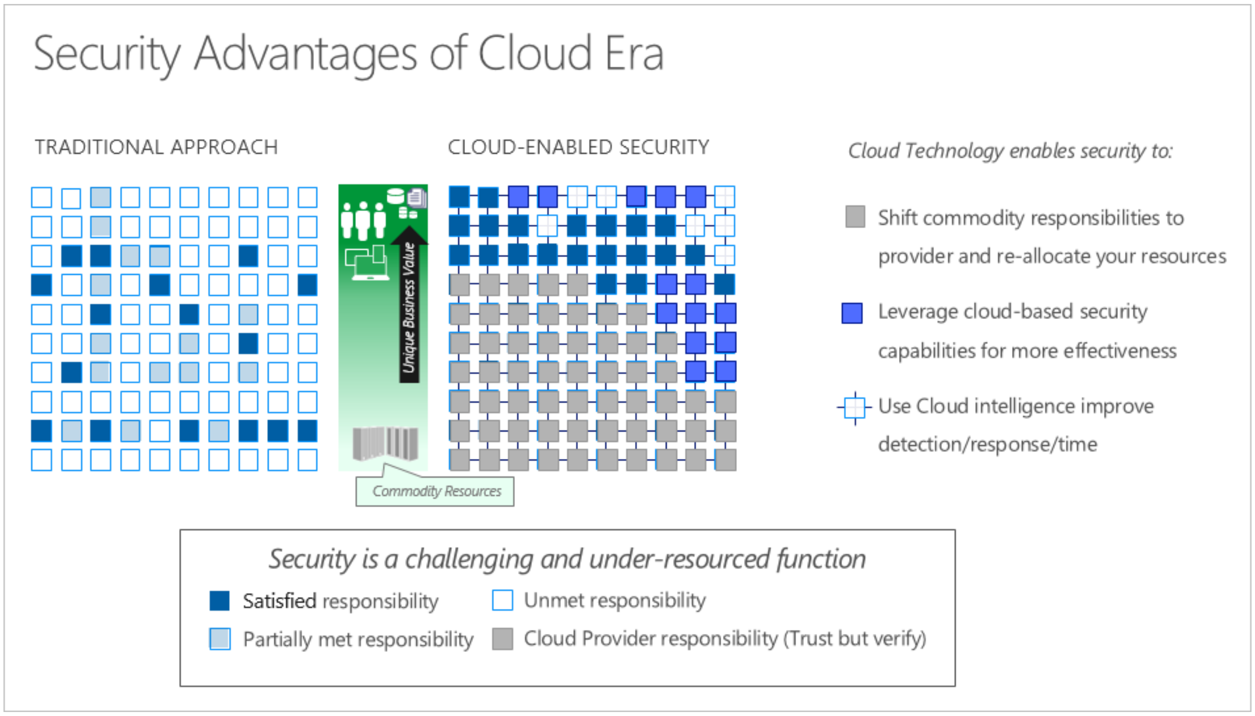
- What the practice is
- Why you want to enable it
- What might be the result if you don’t enable it
- How you can learn to enable it
- Where to find detailed information

Table of Contents

Overview

Most consider the cloud to be more secure than corporate datacenters, as shown in the following figure. Organizations face many challenges with securing their datacenters, including recruiting and keeping security experts, using many security tools, and keeping pace with the volume and complexity of threats.

Azure is uniquely positioned to help organizations with these challenges. Azure helps protect business assets while reducing security costs and complexity. Built-in security controls and intelligence help admins easily identify and respond to threats and security gaps, so organizations can rapidly improve their security posture. By shifting responsibilities to Azure, organizations can get more security coverage—which enables them to move security resources and budget to other business priorities.


Security Advantages of Cloud Era
TRADITIONAL APPROACH
CLOUD-ENABLED SECURITY
Unique Business Value
Commodity Resources
Cloud Technology enables security to:
Shift commodity responsibilities to provider and re-allocate your resources
Leverage cloud-based security capabilities for more effectiveness
Use Cloud intelligence improve detection/response/time
Security is a challenging and under-resourced function
Satisfied responsibility
Unmet responsibility
Partially met responsibility
Cloud Provider responsibility (Trust but verify)

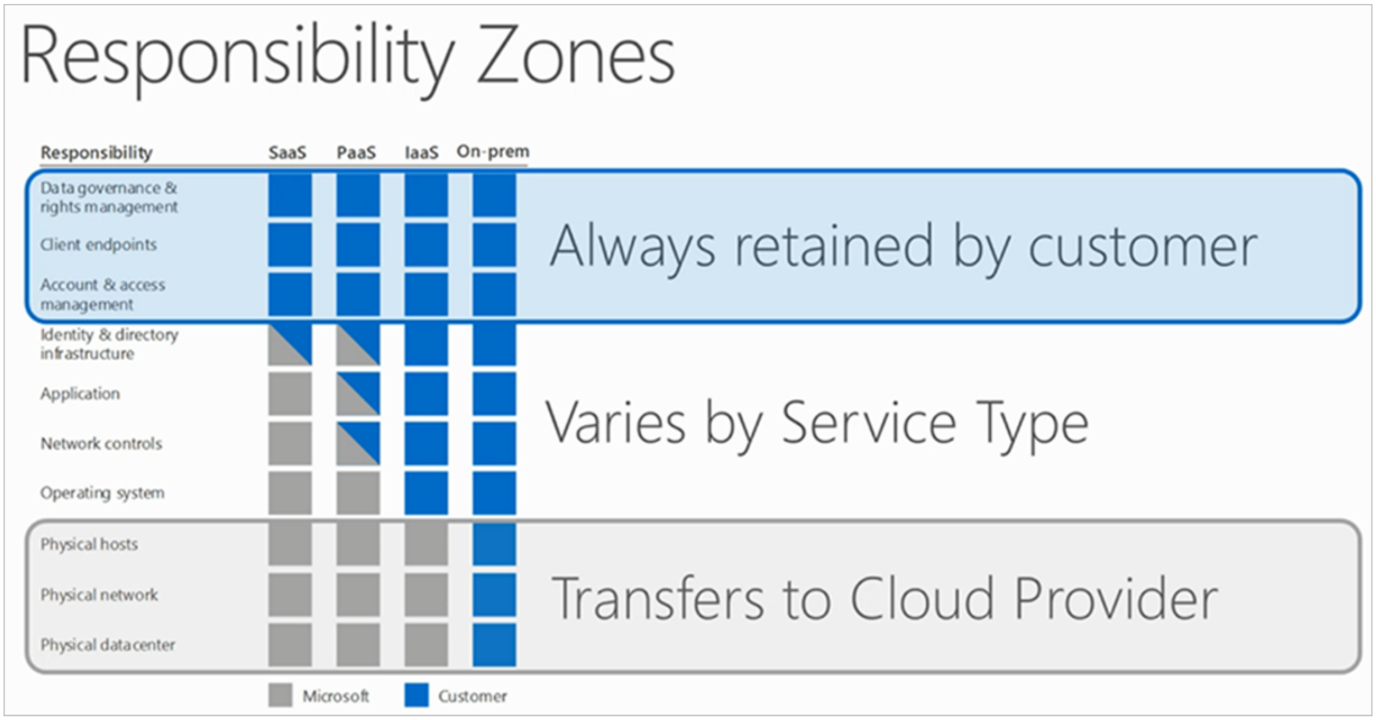
Understand the shared responsibility model for the cloud

It's important to understand the division of responsibility between you and Microsoft. On-premises, you own the whole stack. But as you move to the cloud, some responsibilities transfer to Microsoft.

Microsoft provides a secure foundation across physical, infrastructure, and operational security. Physical security refers to how Microsoft takes a multilayered approach to protect its datacenters. Network infrastructure, firmware and hardware, and continuous testing and monitoring make up the Azure infrastructure. Operational security consists of different security teams at Microsoft that work to mitigate risks across the security landscape.

The following figure shows the areas of the stack on-premises and in a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) deployment that you and Microsoft are responsible for.

© 2018, Microsoft Corporation



For all cloud deployment types, you are responsible for protecting the security of your data, identities, on-premises resources, and the cloud components that you control (which vary by service type). Responsibilities that you always keep, regardless of the type of deployment, are:

- Data
- Endpoints
- Account
- Access management

Be sure that you understand the division of responsibility between you and Microsoft in a SaaS, PaaS, and IaaS deployment. For more details on the division of responsibility, see Shared Responsibilities for Cloud Computing.

Classify your data for cloud readiness

Classifying your data and identifying your data protection needs help you select the right cloud solution for your organization. Classifying (categorizing) stored data by sensitivity and business impact helps organizations determine the risks associated with the data. After the process is completed, organizations can manage their data in ways that reflect its value to them instead of treating all data the same way. Data classification enables organizations to find optimizations that might not be possible when all data is assigned the same value.

Data classification can yield benefits like compliance efficiencies, improved ways to manage the organization's resources, and facilitation of migration to the cloud. It's also worth noting that an organization must address data classification rules for data retention when moving to the cloud, and that cloud solutions can help mitigate risk. Some data protection technologies—such as encryption, rights management, and data loss prevention solutions—have moved to the cloud and can help mitigate cloud risks.

© 2018, Microsoft Corporation

The downloadable white paper Data classification for cloud readiness provides guidance on classifying data.

Shared responsibility for compliance

Microsoft provides resources to assist you in building and launching cloud-powered applications that help you comply with stringent regulations and standards. Because Azure has more certifications than any other cloud provider, you can deploy your critical workloads to Azure with confidence.

Recommended resources to help you stay compliant with regulatory standards are:

- Microsoft Azure Blueprints. Provides an automated way to deploy and govern cloud environments in a repeatable manner. A blueprint includes an industry-specific overview and industry-specific guidance, a customer responsibilities matrix, reference architectures with threat models, control implementation matrices, and automation to deploy reference architectures.
- Compliance Manager (in preview). Helps your organization by providing a holistic view of your data protection and compliance posture when you're using Microsoft cloud services. Compliance Manager helps you perform risk assessments and simplifies your compliance process by providing recommended actions, evidence gathering, and audit preparedness. Key features of Compliance Manager are:
  - Risk assessment capabilities, so you can assess your organization's Azure compliance posture for ISO 27001:2013 , HIPAA, and others.
  - Recommended actions that provide rich insight and direction to improve your data protection capabilities and compliance posture.
  - Simplified compliance that streamlines your organization's compliance and auditing workflow with built-in control management and audit-ready reporting tools.

Top security best practices to do now

We understand that you're busy and may not be able to immediately read this entire document. To help you get started fast, here are the top security best practices you can do now to secure your Azure solution:

- Upgrade your Azure subscription to Azure Security Center Standard. Security Center's Standard tier helps you find and fix security vulnerabilities, apply access and application controls to block malicious activity, detect threats using analytics and intelligence, and respond quickly when under attack.
- Store your keys and secrets in Azure Key Vault (and not in your source code). Key Vault is designed to support any type of secret: passwords, database credentials, API keys and, certificates.
- Install a web application firewall. Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities.
- Enforce multi-factor verification for users, especially your administrator accounts. Azure Multi-Factor Authentication (Azure MFA) helps administrators protect their organizations and users with additional authentication methods.

- Encrypt your virtual hard disk files to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets.
- Connect Azure virtual machines and appliances to other networked devices by placing them on Azure virtual networks. Virtual machines connected to an Azure virtual network can connect to devices on the same virtual network, different virtual networks, the internet, or your own on-premises networks.
- Mitigate and protect against DDoS. Distributed denial of service (DDoS) is a type of attack that tries to exhaust application resources. Azure has two DDoS service offerings that help protect your network from attacks. DDoS Protection Basic is automatically enabled as part of the Azure platform. DDoS Protection Standard provides additional mitigation capabilities—beyond those of the Basic service tier—that are tuned specifically to Azure Virtual Network resources.

Strong operational security practices to implement every day are:

- Manage your VM updates. Azure VMs, like all on-premises VMs, are meant to be user managed. Azure doesn't push Windows updates to them. Ensure you have solid processes in place for important operations such as patch management and backup.
- Enable password management and use appropriate security policies to prevent abuse.
- Review your Security Center dashboard regularly to get a central view of the security state of all of your Azure resources and take action on the recommendations.

Optimize identity and access management

Things you can do to optimize identity and access management include:

- Treat identity as the primary security perimeter
- Centralize identity management
- Enable single sign-on
- Turn on conditional access
- Enable password management
- Enforce multi-factor verification for users
- Use role-based access control
- Lower exposure of privileged accounts
- Control locations where resources are located

Treat identity as the primary security perimeter

Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security. Network perimeters keep getting more porous, and that perimeter defense can’t be as effective as it was before the explosion of BYOD devices and cloud applications.

Azure Active Directory (Azure AD) is the Azure solution for identity and access management. Azure AD is a multitenant, cloud-based directory and identity management service from Microsoft. It combines core directory services, application access management, and identity protection into a single solution.

The following sections list best practices for identity and access security using Azure AD.

© 2018, Microsoft Corporation

Centralize identity management

In a hybrid identity scenario, we recommend that you integrate your on-premises and cloud directories. Integration enables your IT team to manage accounts from one location, regardless of where an account is created. Integration also helps your users be more productive by providing a common identity for accessing both cloud and on-premises resources.

Best practice	Solution
Establish a single Azure AD instance. Consistency and a single authoritative source will increase clarity and reduce security risks from human errors and configuration complexity.	Designate a single Azure AD directory as the authoritative source for corporate and organizational accounts.
Integrate your on-premises directories with Azure AD.	Use Azure AD Connect to synchronize your on-premises directory with your cloud directory. **Note:** There are factors that affect the performance of Azure AD Connect. Ensure Azure AD Connect has enough capacity to keep underperforming systems from impeding security and productivity. Large or complex organizations (organizations provisioning more than 100,000 objects) should follow the recommendations to optimize their Azure AD Connect implementation.
Don’t synchronize accounts to Azure AD that have high privileges in your existing Active Directory instance.	Don’t change the default Azure AD Connect configuration that filters out these accounts. This configuration mitigates the risk of adversaries pivoting from cloud to on-premises assets (which could create a major incident).

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

Organizations that don't integrate their on-premises identity with their cloud identity can have more overhead in managing accounts. This overhead increases the likelihood of mistakes and security breaches.

Note: You need to choose which directories critical accounts will reside in and whether the admin workstation used is managed by new cloud services or existing processes. Using existing management and identity provisioning processes can decrease some risks but can also create the risk of an attacker compromising an on-premises account and pivoting to the cloud. You might want to use a different strategy for different roles (for example, IT admins vs. business unit admins). Your options are:

- Create Azure AD Accounts that aren't synchronized with your on-premises Active Directory instance. Join your admin workstation to Azure AD, which you can manage and patch by using Microsoft Intune.
- Use existing admin accounts by synchronizing to your on-premises Active Directory instance. Use existing workstations in your Active Directory domain for management and security.

Manage connected tenants

Your security organization needs visibility to assess risk and to determine whether the policies of your organization, and any regulatory requirements, are being followed. You should ensure that your security organization has visibility into all subscriptions connected to your production environment and network (via Azure ExpressRoute or site-to-site VPN). A Global Administrator/Company Administrator in Azure AD can elevate their access to the User Access Administrator role and see all subscriptions and managed groups connected to your environment.

See elevate access to manage all Azure subscriptions and management groups to ensure that you and your security group can view all subscriptions or management groups connected to your environment. You should remove this elevated access after you've assessed risks.

Enable single sign-on

In a mobile-first, cloud-first world, you want to enable single sign-on (SSO) to devices, apps, and services from anywhere so your users can be productive wherever and whenever. When you have multiple identity solutions to manage, this becomes an administrative problem not only for IT but also for users who have to remember multiple passwords.

By using the same identity solution for all your apps and resources, you can achieve SSO. And your users can use the same set of credentials to sign in and access the resources that they need, whether the resources are located on-premises or in the cloud.

Best practice	**Solution**
Enable SSO.	Azure AD extends on-premises Active Directory to the cloud. Users can use their primary work or school account for their domain-joined devices, company resources, and all of the web and SaaS applications that they need to get their jobs done. Users don't have to remember multiple sets of usernames and passwords, and their application access can be automatically provisioned (or deprovisioned) based on their organization group memberships and their status as an employee. And you can control that access for gallery apps or for your own on-premises apps that you've developed and published through the Azure AD Application Proxy.

© 2018, Microsoft Corporation

Use SSO to enable users to access their SaaS applications based on their work or school account in Azure AD. This is applicable not only for Microsoft SaaS apps, but also other apps, such as Google Apps and Salesforce. You can configure your application to use Azure AD as a SAML-based identity provider. As a security control, Azure AD does not issue a token that allows users to sign into the application unless they have been granted access through Azure AD. You can grant access directly, or through a group that users are a member of.

Organizations that don't create a common identity to establish SSO for their users and applications are more exposed to scenarios where users have multiple passwords. These scenarios increase the likelihood of users reusing passwords or using weak passwords.

Turn on conditional access

Users can access your organization's resources by using a variety of devices and apps from anywhere. As an IT admin, you want to make sure that these devices meet your standards for security and compliance. Just focusing on who can access a resource isn't sufficient anymore.

To balance security and productivity, you need to think about how a resource is accessed before you can make a decision about access control. With Azure AD conditional access, you can address this requirement. With conditional access, you can make automated access control decisions—based on conditions—for accessing your cloud apps.

Best practice	Solution
Manage and control access to corporate resources.	Configure Azure AD conditional access based on a group, location, and application sensitivity for SaaS apps and Azure AD–connected apps.
Block legacy authentication protocols.	Attackers exploit weaknesses in older protocols every day, particularly for password spray attacks. Configure conditional access to block legacy protocols. See the video Azure AD: Do's and Don'ts for more information.

Enable password management

If you have multiple tenants or you want to enable users to reset their own passwords, it's important that you use appropriate security policies to prevent abuse.

Best practice	Solution
Set up self-service password reset (SSPR) for your users.	Use the Azure AD self-service password reset feature.
Monitor how or if SSPR is really being used.	Monitor the users who are registering by using the Azure AD Password Reset Registration Activity report. The reporting feature that Azure AD provides helps you answer questions by

© 2018, Microsoft Corporation

Best practice	Solution
	using prebuilt reports. If you're appropriately licensed, you can also create custom queries.
Extend cloud-based password policies to your on-premises infrastructure.	Enhance password policies in your organization by performing the same checks for on-premises password changes as you do for cloud-based password changes. Install Azure AD password protection for Windows Server Active Directory agents on-premises to extend banned password lists to your existing infrastructure. Users and admins who change, set, or reset passwords on-premises are required to comply with the same password policy as cloud-only users.

Enforce multi-factor verification for users

We recommend that you require two-step verification for all of your users. This includes administrators and others in your organization who can have a significant impact if their account is compromised (for example, financial officers).

There are multiple options for requiring two-step verification. The best option for you depends on your goals, the Azure AD edition you're running, and your licensing program. See How to require two-step verification for a user to determine the best option for you. See the Azure AD and Azure Multi-Factor Authentication pricing pages for more information about licenses and pricing.

The following table describes options and benefits for enabling two-step verification:

Option	Benefits
Option 1: Enable Multi-Factor Authentication by changing user state	This is the traditional method for requiring two-step verification. It works with both Azure Multi-Factor Authentication in the cloud and Azure Multi-Factor Authentication Server. Using this method requires users to perform two-step verification every time they sign in and overrides conditional access policies. To determine where Multi-Factor Authentication needs to be enabled, see Which version of Azure MFA is right for my organization?.
Option 2: Enable Multi-Factor Authentication with conditional access policy	This option allows you to prompt for two-step verification under specific conditions by using conditional access. Specific conditions can be user sign-in from different locations, untrusted

Option	Benefits
	devices, or applications that you consider risky. Defining specific conditions where you require two-step verification enables you to avoid constant prompting for your users, which can be an unpleasant user experience. This is the most flexible way to enable two-step verification for your users. Enabling a conditional access policy works only for Azure Multi-Factor Authentication in the cloud and is a premium feature of Azure AD. You can find more information on this method in Deploy cloud-based Azure Multi-Factor Authentication.
Option 3: Enable Multi-Factor Authentication with conditional access policies by evaluating user and sign-in risk of Azure AD Identity Protection	This option enables you to: • Detect potential vulnerabilities that affect your organization's identities. • Configure automated responses to detected suspicious actions that are related to your organization's identities. • Investigate suspicious incidents and take appropriate action to resolve them. This method uses the Azure AD Identity Protection risk evaluation to determine if two-step verification is required based on user and sign-in risk for all cloud applications. This method requires Azure Active Directory P2 licensing. You can find more information on this method in Azure Active Directory Identity Protection.

Note: Option 1, enabling Multi-Factor Authentication by changing the user state, overrides conditional policies. Because options 2 and 3 use conditional access policies, you cannot use option 1 with them.

Organizations that don't add extra layers of identity protection, such as two-step verification, are more susceptible for credential theft attack. A credential theft attack can lead to data compromise.

Use role-based access control

Access management for cloud resources is critical for any organization that uses the cloud. Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Designating groups or individual roles responsible for specific functions in Azure helps avoid confusion that can lead to human and automation errors that create security risks. Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.

Your security team needs visibility into your Azure resources in order to assess and remediate risk. If the security team has operational responsibilities, they need additional permissions to do their jobs.

You can use RBAC to assign permissions to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource.

Best practices for using RBAC to manage access to your cloud resources are:

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

Best practice	Solution
security teams to quickly identify and remediate risks.	security policies, view security states, edit security policies, view alerts and recommendations, and dismiss alerts and recommendations. You can do this by using the root management group or the segment management group, depending on the scope of responsibilities.

Organizations that don't enforce data access control by using capabilities like RBAC might be giving more privileges than necessary to their users. This can lead to data compromise by allowing users to access types of data (for example, high business impact) that they shouldn't have.

Lower exposure of privileged accounts

Securing privileged access is a critical first step to protecting business assets. Minimizing the number of people who have access to secure information or resources reduces the chance of a malicious user getting access, or an authorized user inadvertently affecting a sensitive resource.

Privileged accounts are accounts that administer and manage IT systems. Cyber attackers target these accounts to gain access to an organization's data and systems. To secure privileged access, you should isolate the accounts and systems from the risk of being exposed to a malicious user.

We recommend that you develop and follow a roadmap to secure privileged access against cyber attackers. For information about creating a detailed roadmap to secure identities and access that are managed or reported in Azure AD, Microsoft Azure, Office 365, and other cloud services, review Securing privileged access for hybrid and cloud deployments in Azure AD.

Best practices for lowering exposure to privileged accounts are:

Best practice	Solution
Manage, control, and monitor access to privileged accounts.	Turn on Azure AD Privileged Identity Management. After you turn on Privileged Identity Management, you'll receive notification email messages for privileged access role changes. These notifications provide early warning when additional users are added to highly privileged roles in your directory.
Ensure all critical admin accounts are managed Azure AD accounts.	Remove any consumer accounts from critical admin roles (for example, Microsoft accounts like @hotmail.com, @live.com, and @outlook.com).
Ensure all critical admin roles have a separate account for administrative tasks in order to	Create a separate admin account that's assigned the privileges needed to perform the administrative tasks. Block the use of these

© 2018, Microsoft Corporation

Best practice	Solution
avoid phishing and other attacks to compromise administrative privileges.	administrative accounts for daily productivity tools like Microsoft Office 365 email or arbitrary web browsing.
Identify and categorize accounts that are in highly privileged roles.	After turning on Azure AD Privileged Identity Management, view the users who are in the global administrator, privileged role administrator, and other highly privileged roles. Remove any accounts that are no longer needed in those roles, and categorize the remaining accounts that are assigned to admin roles: • Individually assigned to administrative users, and can be used for non-administrative purposes (for example, personal email) • Individually assigned to administrative users and designated for administrative purposes only • Shared across multiple users • For emergency access scenarios • For automated scripts • For external users
Implement "just in time" (JIT) access to further lower the exposure time of privileges and increase your visibility into the use of privileged accounts.	Azure AD Privileged Identity Management lets you: • Limit users to only taking on their privileges JIT. • Assign roles for a shortened duration with confidence that the privileges are revoked automatically.
Define at least two emergency access accounts.	Emergency access accounts help organizations restrict privileged access in an existing Azure Active Directory environment. These accounts are highly privileged and are not assigned to specific individuals. Emergency access accounts are limited to scenarios where normal administrative accounts can't be used. Organizations must limit the emergency account's usage to only the necessary amount of time. Evaluate the accounts that are assigned or eligible for the global admin role. If you don't see any cloud-only accounts by using the

Best practice	Solution
	*.onmicrosoft.com domain (intended for emergency access), create them. For more information, see Managing emergency access administrative accounts in Azure AD.
Have a "break glass" process in place in case of an emergency.	Follow the steps in Securing privileged access for hybrid and cloud deployments in Azure AD.
Require all critical admin accounts to be password-less (preferred), or require Multi-Factor Authentication.	Use the Microsoft Authenticator app to sign in to any Azure AD account without using a password. Like Windows Hello for Business, the Microsoft Authenticator uses key-based authentication to enable a user credential that's tied to a device and uses biometric authentication or a PIN. Require Azure Multi-Factor Authentication at sign-in for all individual users who are permanently assigned to one or more of the Azure AD admin roles: Global Administrator, Privileged Role Administrator, Exchange Online Administrator, and SharePoint Online Administrator. Enable Multi-Factor Authentication for your admin accounts and ensure that admin account users have registered.
For critical admin accounts, have an admin workstation where production tasks aren't allowed (for example, browsing and email). This will protect your admin accounts from attack vectors that use browsing and email and significantly lower your risk of a major incident.	Use an admin workstation. Choose a level of workstation security: • Highly secure productivity devices provide advanced security for browsing and other productivity tasks. • Privileged Access Workstations (PAWs) provide a dedicated operating system that's protected from internet attacks and threat vectors for sensitive tasks.
Deprovision admin accounts when employees leave your organization.	Have a process in place that disables or deletes admin accounts when employees leave your organization.
Regularly test admin accounts by using current attack techniques.	Use Office 365 Attack Simulator or a third-party offering to run realistic attack scenarios in your organization. This can help you find vulnerable users before a real attack occurs.

Best practice	Solution
Take steps to mitigate the most frequently used attacked techniques.	Identify Microsoft accounts in administrative roles that need to be switched to work or school accounts Ensure separate user accounts and mail forwarding for global administrator accounts Ensure that the passwords of administrative accounts have recently changed Turn on password hash synchronization Require Multi-Factor Authentication for users in all privileged roles as well as exposed users Obtain your Office 365 Secure Score (if using Office 365) Review the Office 365 security and compliance guidance (if using Office 365) Configure Office 365 Activity Monitoring (if using Office 365) Establish incident/emergency response plan owners Secure on-premises privileged administrative accounts

If you don’t secure privileged access, you might find that you have too many users in highly privileged roles and are more vulnerable to attacks. Malicious actors, including cyber attackers, often target admin accounts and other elements of privileged access to gain access to sensitive data and systems by using credential theft.

Control locations where resources are created

Enabling cloud operators to perform tasks while preventing them from breaking conventions that are needed to manage your organization's resources is very important. Organizations that want to control the locations where resources are created should hard code these locations.

You can use Azure Resource Manager to create security policies whose definitions describe the actions or resources that are specifically denied. You assign those policy definitions at the desired scope, such as the subscription, the resource group, or an individual resource.

Note: Security policies are not the same as RBAC. They actually use RBAC to authorize users to create those resources.

Organizations that are not controlling how resources are created are more susceptible to users who might abuse the service by creating more resources than they need. Hardening the resource creation process is an important step to securing a multitenant scenario.

Actively monitor for suspicious activities

An active identity monitoring system can quickly detect suspicious behavior and trigger an alert for further investigation. The following table lists two Azure AD capabilities that can help organizations monitor their identities:

Best practice	Solution
Have a method to identify: • Attempts to sign in without being traced. • Brute force attacks against a particular account. • Attempts to sign in from multiple locations. • Sign-ins from infected devices. • Suspicious IP addresses.	Use Azure AD Premium anomaly reports. Have processes and procedures in place for IT admins to run these reports on a daily basis or on demand (usually in an incident response scenario).
Have an active monitoring system that notifies you of risks and can adjust risk level (high, medium, or low) to your business requirements.	Use Azure AD Identity Protection, which flags the current risks on its own dashboard and sends daily summary notifications via email. To help protect your organization's identities, you can configure risk-based policies that automatically respond to detected issues when a specified risk level is reached.

Organizations that don’t actively monitor their identity systems are at risk of having user credentials compromised. Without knowledge that suspicious activities are taking place through these credentials, organizations can’t mitigate this type of threat.

Use Azure AD for storage authentication

Azure Storage supports authentication and authorization with Azure AD for Blob storage and Queue storage. With Azure AD authentication, you can use Azure role-based access control to grant specific permissions to users, groups, and applications—down to the scope of an individual blob container or queue.

We recommend that you use Azure AD for authenticating access to storage.

Use strong network controls

You can connect Azure virtual machines (VMs) and appliances to other networked devices by placing them on Azure virtual networks. That is, you can connect virtual network interface cards to a virtual network to allow TCP/IP-based communications between network-enabled devices. Virtual machines connected to an Azure virtual network can connect to devices on the same virtual network, different virtual networks, the internet, or your own on-premises networks.

As you plan your network and the security of your network, we recommend that you centralize:

- Management of core network functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing.
- Governance of network security elements, such as network virtual appliance functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing.

If you use a common set of management tools to monitor your network and the security of your network, you get clear visibility into both. A straightforward, unified security strategy reduces errors because it increases human understanding and the reliability of automation.

The following sections describe best practices for network security.

Logically segment subnets

Azure virtual networks are similar to LANs on your on-premises network. The idea behind an Azure virtual network is that you create a network, based on a single private IP address space, on which you can place all your Azure virtual machines. The private IP address spaces available are in the Class A (10.0.0.0/8), Class B (172.16.0.0/12), and Class C (192.168.0.0/16) ranges.

Best practices for logically segmenting subnets include:

Best practice	Solution
Don’t assign allow rules with broad ranges (for example, allow 0.0.0.0 through 255.255.255.255).	Ensure troubleshooting procedures discourage or ban setting up these types of rules. These allow rules lead to a false sense of security and are frequently found and exploited by red teams.
Segment the larger address space into subnets.	Use CIDR-based subnetting principles to create your subnets.
Create network access controls between subnets. Routing between subnets happens automatically, and you don’t need to manually configure routing tables. By default, there are no network access controls between the subnets that you create on an Azure virtual network.	Use a network security group to protect against unsolicited traffic into Azure subnets. Network security groups are simple, stateful packet inspection devices that use the 5-tuple approach (source IP, source port, destination IP, destination port, and layer 4 protocol) to create allow/deny rules for network traffic. You allow or deny traffic to and from a single IP address, to and from multiple IP addresses, or to and from entire subnets. When you use network security groups for network access control between subnets, you can put resources that belong to the same security zone or role in their own subnets.
Avoid small virtual networks and subnets to ensure simplicity and flexibility.	Most organizations add more resources than initially planned, and re-allocating addresses is labor intensive. Using small subnets adds limited security value, and mapping a network

Best practice	Solution
	security group to each subnet adds overhead. Define subnets broadly to ensure that you have flexibility for growth.
Simplify network security group rule management by defining Application Security Groups.	Define an Application Security Group for lists of IP addresses that you think might change in the future or be used across many network security groups. Be sure to name Application Security Groups clearly so others can understand their content and purpose.

Adopt a Zero Trust approach

Perimeter-based networks operate on the assumption that all systems within a network can be trusted. But today's employees access their organization's resources from anywhere on a variety of devices and apps, which makes perimeter security controls irrelevant. Access control policies that focus only on who can access a resource are not enough. To master the balance between security and productivity, security admins also need to factor in *how* a resource is being accessed.

Networks need to evolve from traditional defenses because networks might be vulnerable to breaches: an attacker can compromise a single endpoint within the trusted boundary and then quickly expand a foothold across the entire network. Zero Trust networks eliminate the concept of trust based on network location within a perimeter. Instead, Zero Trust architectures use device and user trust claims to gate access to organizational data and resources. For new initiatives, adopt Zero Trust approaches that validate trust at the time of access.

Best practices are:

Best practice	Solution
Give conditional access to resources based on device, identity, assurance, network location, and more.	Azure AD conditional access lets you apply the right access controls by implementing automated access control decisions based on the required conditions. For more information, see Manage access to Azure management with conditional access.
Enable port access only after workflow approval.	You can use just-in-time VM access in Azure Security Center to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Grant temporary permissions to perform privileged tasks, which prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it.	Use just-in-time access in Azure AD Privileged Identity Management or in a third-party solution to grant permissions to perform privileged tasks.

Zero Trust is the next evolution in network security. The state of cyberattacks drives organizations to take the "assume breach" mindset, but this approach shouldn't be limiting. Zero Trust networks protect corporate data and resources while ensuring that organizations can build a modern workplace by using technologies that empower employees to be productive anytime, anywhere, in any way.

Control routing behavior

When you put a virtual machine on an Azure virtual network, the VM can connect to any other VM on the same virtual network, even if the other VMs are on different subnets. This is possible because a collection of system routes enabled by default allows this type of communication. These default routes allow VMs on the same virtual network to initiate connections with each other, and with the internet (for outbound communications to the internet only).

Although the default system routes are useful for many deployment scenarios, there are times when you want to customize the routing configuration for your deployments. You can configure the next-hop address to reach specific destinations.

We recommend that you configure user-defined routes when you deploy a security appliance for a virtual network. We talk about this in a later section titled secure your critical Azure service resources to only your virtual networks.

Note: User-defined routes are not required, and the default system routes usually work.

Use virtual network appliances

Network security groups and user-defined routing can provide a certain measure of network security at the network and transport layers of the OSI model. But in some situations, you want or need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances provided by Azure partners.

Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

- Firewalling
- Intrusion detection/intrusion prevention
- Vulnerability management
- Application control
- Network-based anomaly detection
- Web filtering
- Antivirus
- Botnet protection

To find available Azure virtual network security appliances, go to the Azure Marketplace and search for "security" and "network security."

Deploy perimeter networks for security zones

A perimeter network (also known as a DMZ) is a physical or logical network segment that provides an additional layer of security between your assets and the internet. Specialized network access control devices on the edge of a perimeter network allow only desired traffic into your virtual network.

Perimeter networks are useful because you can focus your network access control management, monitoring, logging, and reporting on the devices at the edge of your Azure virtual network. A perimeter network is where you typically enable distributed denial of service (DDoS) prevention, intrusion detection/intrusion prevention systems (IDS/IPS), firewall rules and policies, web filtering, network antimalware, and more. The network security devices sit between the internet and your Azure virtual network and have an interface on both networks.

Although this is the basic design of a perimeter network, there are many different designs, like back-to-back, tri-homed, and multi-homed.

Based on the Zero Trust concept mentioned earlier, we recommend that you consider using a perimeter network for all high security deployments to enhance the level of network security and access control for your Azure resources. You can use Azure or a third-party solution to provide an additional layer of security between your assets and the internet:

- **Azure native controls**. Azure Firewall and the web application firewall in Application Gateway offer basic security with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration.
- Third-party offerings. Search the Azure Marketplace for next-generation firewall (NGFW) and other third-party offerings that provide familiar security tools and significantly enhanced levels of network security. Configuration might be more complex, but a third-party offering might allow you to use existing capabilities and skill sets.

Avoid exposure to the internet with dedicated WAN links

Many organizations have chosen the hybrid IT route. With hybrid IT, some of the company's information assets are in Azure, and others remain on-premises. In many cases, some components of a service are running in Azure while other components remain on-premises.

In a hybrid IT scenario, there's usually some type of cross-premises connectivity. Cross-premises connectivity allows the company to connect its on-premises networks to Azure virtual networks. Two cross-premises connectivity solutions are available:

- **Site-to-site VPN**. It's a trusted, reliable, and established technology, but the connection takes place over the internet. Bandwidth is constrained to a maximum of about 200 Mbps. Site-to-site VPN is a desirable option in some scenarios. It's discussed further in the Disable RDP/SSH access to virtual machines section of this white paper.
- **Azure ExpressRoute**. We recommend that you use ExpressRoute for your cross-premises connectivity. ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services like Azure, Office 365, and Dynamics 365. ExpressRoute is a dedicated WAN link between your on-premises location or a Microsoft Exchange hosting provider. Because this is a telco connection, your data doesn't travel over the internet, so it isn't exposed to the potential risks of internet communications.

  The location of your ExpressRoute connection can affect firewall capacity, scalability, reliability, and network traffic visibility. You'll need to identify where to terminate ExpressRoute in existing (on-premises) networks. You can:

- Terminate outside the firewall (the perimeter network paradigm) if you require visibility into the traffic, if you need to continue an existing practice of isolating datacenters, or if you're solely putting extranet resources on Azure.
- Terminate inside the firewall (the network extension paradigm). This is the default recommendation. In all other cases, we recommend treating Azure as an *n*th datacenter.

Optimize uptime and performance

If a service is down, information can't be accessed. If performance is so poor that the data is unusable, you can consider the data to be inaccessible. From a security perspective, you need to do whatever you can to make sure that your services have optimal uptime and performance.

A popular and effective method for enhancing availability and performance is load balancing. Load balancing is a method of distributing network traffic across servers that are part of a service. For example, if you have front-end web servers as part of your service, you can use load balancing to distribute the traffic across your multiple front-end web servers.

This distribution of traffic increases availability because if one of the web servers becomes unavailable, the load balancer stops sending traffic to that server and redirects it to the servers that are still online. Load balancing also helps performance, because the processor, network, and memory overhead for serving requests is distributed across all the load-balanced servers.

We recommend that you employ load balancing whenever you can, and as appropriate for your services. The following table lists scenarios at both the Azure virtual network level and the global level, along with load-balancing options for each.

Scenario	**Load-balancing option**
You have an application that: • Requires requests from the same user/client session to reach the same back-end virtual machine. Examples of this are shopping cart apps and web mail servers. • Accepts only a secure connection, so unencrypted communication to the server is not an acceptable option. • Requires multiple HTTP requests on the same long-running TCP connection to be routed or load balanced to different back-end servers.	Use Azure Application Gateway, an HTTP web traffic load balancer. Application Gateway supports end-to-end SSL encryption and SSL termination at the gateway. Web servers can then be unburdened from encryption and decryption overhead and traffic flowing unencrypted to the back-end servers.
You need to load balance incoming connections from the internet among your servers located in an Azure virtual network. Scenarios are when you:	Use the Azure portal to create an external load balancer that spreads incoming requests across multiple VMs to provide a higher level of availability.

© 2018, Microsoft Corporation

Scenario	Load-balancing option
• Have stateless applications that accept incoming requests from the internet. • Don’t require sticky sessions or SSL offload. Sticky sessions is a method used with Application Load Balancing, to achieve server-affinity.	
You need to load balance connections from VMs that are not on the internet. In most cases, the connections that are accepted for load balancing are initiated by devices on an Azure virtual network, such as SQL Server instances or internal web servers.	Use the Azure portal to create an internal load balancer that spreads incoming requests across multiple VMs to provide a higher level of availability.
You need global load balancing because you: • Have a cloud solution that is widely distributed across multiple regions and requires the highest level of uptime (availability) possible. • Need the highest level of uptime possible to make sure that your service is available even if an entire datacenter becomes unavailable.	Use Azure Traffic Manager. Traffic Manager makes it possible to load balance connections to your services based on the location of the user. For example, if the user makes a request to your service from the EU, the connection is directed to your services located in an EU datacenter. This part of Traffic Manager global load balancing helps to improve performance because connecting to the nearest datacenter is faster than connecting to datacenters that are far away.

Disable RDP/SSH access to virtual machines

It’s possible to reach Azure virtual machines by using Remote Desktop Protocol (RDP) and the Secure Shell (SSH) protocol. These protocols enable the management VMs from remote locations and are standard in datacenter computing.

The potential security problem with using these protocols over the internet is that attackers can use brute force techniques to gain access to Azure virtual machines. After the attackers gain access, they can use your VM as a launch point for compromising other machines on your virtual network or even attack networked devices outside Azure.

We recommend that you disable direct RDP and SSH access to your Azure virtual machines from the internet. After direct RDP and SSH access from the internet is disabled, you have other options that you can use to access these VMs for remote management.

Scenario	Option
Enable a single user to connect to an Azure virtual network over the internet.	Point-to-site VPN is another term for a remote access VPN client/server connection. After the point-to-site connection is established, the user can use RDP or SSH to connect to any VMs located on the Azure virtual network that the user connected to via point-to-site VPN. This assumes that the user is authorized to reach those VMs. Point-to-site VPN is more secure than direct RDP or SSH connections because the user has to authenticate twice before connecting to a VM. First, the user needs to authenticate (and be authorized) to establish the point-to-site VPN connection. Second, the user needs to authenticate (and be authorized) to establish the RDP or SSH session.
Enable users on your on-premises network to connect to VMs on your Azure virtual network.	A site-to-site VPN connects an entire network to another network over the internet. You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet.
Use a dedicated WAN link to provide functionality similar to the site-to-site VPN.	Use ExpressRoute. It provides functionality similar to the site-to-site VPN. The main differences are: • The dedicated WAN link doesn't traverse the internet. • Dedicated WAN links are typically more stable and perform better.

Secure your critical Azure service resources to only your virtual networks

Use virtual network service endpoints to extend your virtual network private address space, and the identity of your virtual network to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your virtual network to the Azure service always remains on the Microsoft Azure backbone network.

Service endpoints provide the following benefits:

- **Improved security for your Azure service resources**: With service endpoints, Azure service resources can be secured to your virtual network. Securing service resources to a virtual network provides improved security by fully removing public internet access to resources, and allowing traffic only from your virtual network.
- **Optimal routing for Azure service traffic from your virtual network**: Any routes in your virtual network that force internet traffic to your on-premises and/or virtual appliances, known as forced tunneling, also force Azure service traffic to take the same route as the internet traffic. Service endpoints provide optimal routing for Azure traffic.

  Endpoints always take service traffic directly from your virtual network to the service on the Azure backbone network. Keeping traffic on the Azure backbone network allows you to continue auditing and monitoring outbound internet traffic from your virtual networks, through forced tunneling, without affecting service traffic. Learn more about user-defined routes and forced tunneling.

- **Simple to set up with less management overhead**: You no longer need reserved, public IP addresses in your virtual networks to secure Azure resources through an IP firewall. There are no NAT or gateway devices required to set up the service endpoints. Service endpoints are configured through a simple click on a subnet. There is no additional overhead to maintain the endpoints.

To learn more about service endpoints and the Azure services and regions that service endpoints are available for, see Virtual network service endpoints.

Lock down and secure VM and computer operating systems

In most IaaS scenarios, Azure virtual machines are the main workload for organizations that use cloud computing. This fact is evident in hybrid scenarios where organizations want to slowly migrate workloads to the cloud. In such scenarios, follow the general security considerations for IaaS, and apply security best practices to all your VMs.

The following sections describe security best practices for VMs and operating systems.

Protect VMs by using authentication and access control

For the topics of identity and access, we discussed using strong authentication and authorization to protect data and resources. The first step in protecting your VMs is to ensure that only authorized users can set up new VMs and access VMs.

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

Best practice	**Solution**
Control VM access.	Use Azure policies to establish conventions for resources in your organization and create customized policies. Apply these policies to resources, such as resource groups. VMs that belong to a resource group inherit its policies. If your organization has many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into management groups (containers) and apply your governance conditions to those groups. All subscriptions within a management group automatically inherit the conditions applied to the group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have.

Best practice	Solution
Reduce variability in your setup and deployment of VMs.	Use Azure Resource Manager templates to strengthen your deployment choices and make it easier to understand and inventory the VMs in your environment.
Secure privileged access.	Use a least privilege approach and built-in Azure roles to enable users to access and set up VMs: • Virtual Machine Contributor: Can manage VMs, but not the virtual network or storage account to which they are connected. • Classic Virtual Machine Contributor: Can manage VMs created by using the classic deployment model, but not the virtual network or storage account to which the VMs are connected. • Security Manager: Can manage security components, security policies, and VMs. • DevTest Labs User: Can view everything and connect, start, restart, and shut down VMs. **Note:** Your subscription admins and coadmins can change this setting, making them administrators of all the VMs in a subscription. Be sure that you trust all of your subscription admins and coadmins to log in to any of your machines.

Note: We recommend that you consolidate VMs with the same lifecycle into the same resource group. By using resource groups, you can deploy, monitor, and roll up billing costs for your resources.

Organizations that control VM access and setup improve their overall VM security.

Use multiple VMs for better availability

If your VM runs critical applications that need to have high availability, we strongly recommend that you use multiple VMs. For better availability, use an availability set.

An availability set is a logical grouping that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they're deployed in an Azure datacenter. Azure ensures that the VMs you place in an availability set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or Azure software failure occurs, only a subset of your VMs are affected, and your overall application continues to be available to your customers. Availability sets are an essential capability when you want to build reliable cloud solutions.

Protect against malware

You should install antimalware protection to help identify and remove viruses, spyware, and other malicious software. You can install Microsoft Antimalware or a Microsoft partner's endpoint protection solution (Trend Micro, Symantec, McAfee, Windows Defender, and System Center Endpoint Protection).

Microsoft Antimalware includes features like real-time protection, scheduled scanning, malware remediation, signature updates, engine updates, samples reporting, and exclusion event collection. For environments that are hosted separately from your production environment, you can use an antimalware extension to help protect your VMs and cloud services.

You can integrate Microsoft Antimalware and partner solutions with Azure Security Center for ease of deployment and built-in detections (alerts and incidents).

Best practice	Solution
Install an antimalware solution to protect against malware.	Install a Microsoft partner solution or Microsoft Antimalware
Integrate your antimalware solution with Security Center to monitor the status of your protection.	Manage endpoint protection issues with Security Center

Manage your VM updates

Azure VMs, like all on-premises VMs, are meant to be user managed. Azure doesn't push Windows updates to them. You need to manage your VM updates.

Best practice	Solution
Keep your VMs current.	Use the Update Management solution in Azure Automation to manage operating system updates for your Windows and Linux computers that are deployed in Azure, in on-premises environments, or in other cloud providers. You can quickly assess the status of available updates on all agent computers and manage the process of installing required updates for servers. Computers that are managed by Update Management use the following configurations to perform assessment and update deployments: • Microsoft Monitoring Agent (MMA) for Windows or Linux • PowerShell Desired State Configuration (DSC) for Linux • Automation Hybrid Runbook Worker • Microsoft Update or Windows Server Update Services (WSUS) for Windows computers

© 2018, Microsoft Corporation

Best practice	Solution
	Note: If you use Windows Update, leave the automatic Windows Update setting enabled.
Ensure at deployment that images you built include the most recent round of Windows updates.	Check for and install all Windows updates as a first step of every deployment. This measure is especially important to apply when you deploy images that come from either you or your own library. Although images from the Azure Marketplace are updated automatically by default, there can be a lag time (up to a few weeks) after a public release.
Periodically redeploy your VMs to force a fresh version of the OS.	Define your VM with an Azure Resource Manager template so you can easily redeploy it. Using a template gives you a patched and secure VM when you need it.
Rapidly apply security updates to VMs	Enable Azure Security Center (Free tier or Standard tier) to identify missing security updates and apply them.
Deploy and test a backup solution.	A backup needs to be handled the same way that you handle any other operation. This is true of systems that are part of your production environment extending to the cloud. Test and dev systems must follow backup strategies that provide restore capabilities that are similar to what users have grown accustomed to, based on their experience with on-premises environments. Production workloads moved to Azure should integrate with existing backup solutions when possible. Or, you can use Azure Backup to help address your backup requirements.

Organizations that don't enforce software-update policies are more exposed to threats that exploit known, previously fixed vulnerabilities. To comply with industry regulations, companies must prove that they are diligent and using correct security controls to help ensure the security of their workloads located in the cloud.

Software-update best practices for a traditional datacenter and Azure IaaS have many similarities. We recommend that you evaluate your current software update policies to include VMs located in Azure.

Manage your VM security posture

Cyberthreats are evolving. Safeguarding your VMs requires a monitoring capability that can quickly detect threats, prevent unauthorized access to your resources, trigger alerts, and reduce false positives.

To monitor the security posture of your Windows and Linux VMs, use Azure Security Center. In Security Center, safeguard your VMs by taking advantage of the following capabilities:

- Apply OS security settings with recommended configuration rules.
- Identify and download system security and critical updates that might be missing.
- Deploy recommendations for endpoint antimalware protection.
- Validate disk encryption.
- Assess and remediate vulnerabilities.
- Detect threats.

Security Center can actively monitor for threats, and potential threats are exposed in security alerts. Correlated threats are aggregated in a single view called a security incident.

Security Center stores data in Azure Log Analytics. Log Analytics provides a query language and analytics engine that gives you insights into the operation of your applications and resources. Data is also collected from Azure Monitor, management solutions, and agents installed on virtual machines in the cloud or on-premises. This shared functionality helps you form a complete picture of your environment.

Organizations that don't enforce strong security for their VMs remain unaware of potential attempts by unauthorized users to circumvent security controls.

Monitor VM performance

Resource abuse can be a problem when VM processes consume more resources than they should. Performance issues with a VM can lead to service disruption, which violates the security principle of availability. This is particularly important for VMs that are hosting IIS or other web servers, because high CPU or memory usage might indicate a denial of service (DoS) attack. It's imperative to monitor VM access not only reactively while an issue is occurring, but also proactively against baseline performance as measured during normal operation.

We recommend that you use Azure Monitor to gain visibility into your resource's health. Azure Monitor features:

- Resource diagnostic log files: Monitors your VM resources and identifies potential issues that might compromise performance and availability.
- Azure Diagnostics extension: Provides monitoring and diagnostics capabilities on Windows VMs. You can enable these capabilities by including the extension as part of the Azure Resource Manager template.

Organizations that don't monitor VM performance can't determine whether certain changes in performance patterns are normal or abnormal. A VM that's consuming more resources than normal might indicate an attack from an external resource or a compromised process running in the VM.

Encrypt your virtual hard disk files

We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets.

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

The following table lists best practices for using Azure Disk Encryption:

Best practice	Solution
Enable encryption on VMs.	Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication. Create an Azure AD application for this purpose. For authentication purposes, you can use either client secret-based authentication or client certificate-based Azure AD authentication.
Use a key encryption key (KEK) for an additional layer of security for encryption keys. Add a KEK to your key vault.	Use the Add-AzureKeyVaultKey cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises hardware security module (HSM) for key management. For more information, see the Key Vault documentation. When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to Key Vault. Keeping an escrow copy of this key in an on-premises key management HSM offers additional protection against accidental deletion of keys.
Take a snapshot and/or backup before disks are encrypted. Backups provide a recovery option if an unexpected failure happens during encryption.	VMs with managed disks require a backup before encryption occurs. After a backup is made, you can use the **Set-AzureRmVMDiskEncryptionExtension** cmdlet to encrypt managed disks by specifying the *-skipVmBackup* parameter. For more information about how to back up and restore encrypted VMs, see the Azure Backup article.
To make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the key vault and the VMs to be located in the same region.	Create and use a key vault that is in the same region as the VM to be encrypted.

When you apply Azure Disk Encryption, you can satisfy the following business needs:

- IaaS VMs are secured at rest through industry-standard encryption technology to address organizational security and compliance requirements.
- IaaS VMs start under customer-controlled keys and policies, and you can audit their usage in your key vault.

Restrict direct internet connectivity

Monitor and restrict VM direct internet connectivity. Attackers constantly scan public cloud IP ranges for open management ports and attempt "easy" attacks like common passwords and known unpatched vulnerabilities. The following table lists best practices to help protect against these attacks:

Best practice	**Solution**
Prevent inadvertent exposure to network routing and security.	Use RBAC to ensure that only the central networking group has permission to networking resources.
Identify and remediate exposed VMs that allow access from "any" source IP address.	Use Azure Security Center. Security Center will recommend that you restrict access through internet-facing endpoints if any of your network security groups has one or more inbound rules that allow access from "any" source IP address. Security Center will recommend that you edit these inbound rules to restrict access to source IP addresses that actually need access.
Restrict management ports (RDP, SSH)	Just-in-time (JIT) VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. When JIT is enabled, Security Center locks down inbound traffic to your Azure VMs by creating a network security group rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the JIT solution.

Protect data

To help protect data in the cloud, you need to account for the possible states in which your data can occur, and what controls are available for that state. Best practices for Azure data security and encryption relate to the following data states:

- **At rest**: This includes all information storage objects, containers, and types that exist statically on physical media, whether magnetic or optical disk.
- **In transit**: When data is being transferred between components, locations, or programs, it's in transit. Examples are transfer over the network, across a service bus (from on-premises to

cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process.

The following sections describe security best practices for protecting data.

Choose a key management solution

Protecting your keys is essential to protecting your data in the cloud.

Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. Key Vault streamlines the key management process and enables you to maintain control of keys that access and encrypt your data. Developers can create keys for development and testing in minutes, and then migrate them to production keys. Security administrators can grant (and revoke) permission to keys, as needed.

You can use Key Vault to create multiple secure containers, called vaults. These vaults are backed by HSMs. Vaults help reduce the chances of accidental loss of security information by centralizing the storage of application secrets. Key vaults also control and log the access to anything stored in them. Azure Key Vault can handle requesting and renewing Transport Layer Security (TLS) certificates. It provides features for a robust solution for certificate lifecycle management.

Azure Key Vault is designed to support application keys and secrets. Key Vault is not intended to be a store for user passwords.

The following table lists security best practices for using Key Vault:

Best practice	Solution
Grant access to users, groups, and applications at a specific scope.	Use RBAC's predefined roles. For example, to grant access to a user to manage key vaults, you would assign the predefined role Key Vault Contributor to this user at a specific scope. The scope in this case would be a subscription, a resource group, or just a specific key vault. If the predefined roles don't fit your needs, you can define your own roles.
Control what users have access to.	Access to a key vault is controlled through two separate interfaces: management plane and data plane. The management plane and data plane access controls work independently. Use RBAC to control what users have access to. For example, if you want to grant an application access to use keys in a key vault, you only need to grant data plane access permissions by using key vault access policies, and no management plane access is needed for this application. Conversely, if you want a user to be able to read vault properties and tags but not have any access to keys, secrets, or certificates, you can

Best practice	Solution
	grant this user read access by using RBAC, and no access to the data plane is required.
Store certificates in your key vault. Your certificates are of high value. In the wrong hands, your application's security or the security of your data can be compromised.	Azure Resource Manager can securely deploy certificates stored in Azure Key Vault to Azure VMs when the VMs are deployed. By setting appropriate access policies for the key vault, you also control who gets access to your certificate. Another benefit is that you manage all your certificates in one place in Azure Key Vault. See Deploy Certificates to VMs from customer-managed Key Vault for more information.
Ensure that you can recover a deletion of key vaults or key vault objects.	Deletion of key vaults or key vault objects can be inadvertent or malicious. Enable the soft delete and purge protection features of Key Vault, particularly for keys that are used to encrypt data at rest. Deletion of these keys is equivalent to data loss, so you can recover deleted vaults and vault objects if needed. Practice Key Vault recovery operations on a regular basis.

Note: If a user has contributor permissions (RBAC) to a key vault management plane, they can grant themselves access to the data plane by setting a key vault access policy. We recommend that you tightly control who has contributor access to your key vaults, to ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Manage with secure workstations

Note: The subscription administrator or owner should use a secure access workstation or a privileged access workstation.

Because the vast majority of attacks target the end user, the endpoint becomes one of the primary points of attack. An attacker who compromises the endpoint can use the user’s credentials to gain access to the organization’s data. Most endpoint attacks take advantage of the fact that users are administrators in their local workstations.

Best practice	Solution
Use a secure management workstation to protect sensitive accounts, tasks, and data.	Use a privileged access workstation to reduce the attack surface in workstations. These secure management workstations can help you mitigate some of these attacks and ensure that your data is safer.
Ensure endpoint protection.	Enforce security policies across all devices that are used to consume data, regardless of the data location (cloud or on-premises).

Protect data at rest

Data encryption at rest is a mandatory step toward data privacy, compliance, and data sovereignty.

Best practice	Solution
Apply disk encryption to help safeguard your data.	Use Azure Disk Encryption. It enables IT administrators to encrypt Windows and Linux IaaS VM disks. Disk Encryption combines the industry-standard Windows BitLocker feature and the Linux dm-crypt feature to provide volume encryption for the OS and the data disks. Azure Storage and Azure SQL Database encrypt data at rest by default, and many services offer encryption as an option. You can use Azure Key Vault to maintain control of keys that access and encrypt your data. See Azure resource providers encryption model support to learn more.
Use encryption to help mitigate risks related to unauthorized data access.	Encrypt your drives before you write sensitive data to them.

Organizations that don’t enforce data encryption are more exposed to data-integrity issues. For example, unauthorized or rogue users might steal data in compromised accounts or gain unauthorized access to data coded in Clear Format. Companies also must prove that they are diligent and using correct security controls to enhance their data security in order to comply with industry regulations.

Protect data in transit

Protecting data in transit should be an essential part of your data protection strategy. Because data is moving back and forth from many locations, we generally recommend that you always use SSL/TLS protocols to exchange data across different locations. In some circumstances, you might want to isolate the entire communication channel between your on-premises and cloud infrastructures by using a VPN.

For data moving between your on-premises infrastructure and Azure, consider appropriate safeguards such as HTTPS or VPN. When sending encrypted traffic between an Azure virtual network and an on-premises location over the public internet, use Azure VPN Gateway.

The following table lists best practices specific to using Azure VPN Gateway, SSL/TLS, and HTTPS:

Best practice	Solution
Secure access from multiple workstations located on-premises to an Azure virtual network.	Use site-to-site VPN.
Secure access from an individual workstation located on-premises to an Azure virtual network.	Use point-to-site VPN.
Move larger data sets over a dedicated high-speed WAN link.	Use ExpressRoute. If you choose to use ExpressRoute, you can also encrypt the data at the application level by using SSL/TLS or other protocols for added protection.
Interact with Azure Storage through the Azure portal.	All transactions occur via HTTPS. You can also use Storage REST API over HTTPS to interact with Azure Storage.

Organizations that fail to protect data in transit are more susceptible to man-in-the-middle attacks, eavesdropping, and session hijacking. These attacks can be the first step in gaining access to confidential data.

Secure email, documents, and sensitive data

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

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

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

This information protection solution keeps you in control of your data, even when it's shared with other people. You can also use Azure RMS with your own line-of-business applications and information protection solutions from software vendors, whether these applications and solutions are on-premises or in the cloud.

We recommend that you:

- Deploy Azure Information Protection for your organization.
- Apply labels that reflect your business requirements. For example: Apply a label named "highly confidential" to all documents and emails that contain top-secret data, to classify and protect this data. Then, only authorized users can access this data, with any restrictions that you specify.
- Configure usage logging for Azure RMS so that you can monitor how your organization is using the protection service.

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

Secure databases

Security is a top concern for managing databases, and it has always been a priority for Azure SQL Database. Your databases can be tightly secured to help satisfy most regulatory or security requirements, including HIPAA, ISO 27001/27002, and PCI DSS Level 1. A current list of security compliance certifications is available at the Microsoft Trust Center site. You also can choose to place your databases in specific Azure datacenters based on regulatory requirements.

The following sections list best practices for securing databases.

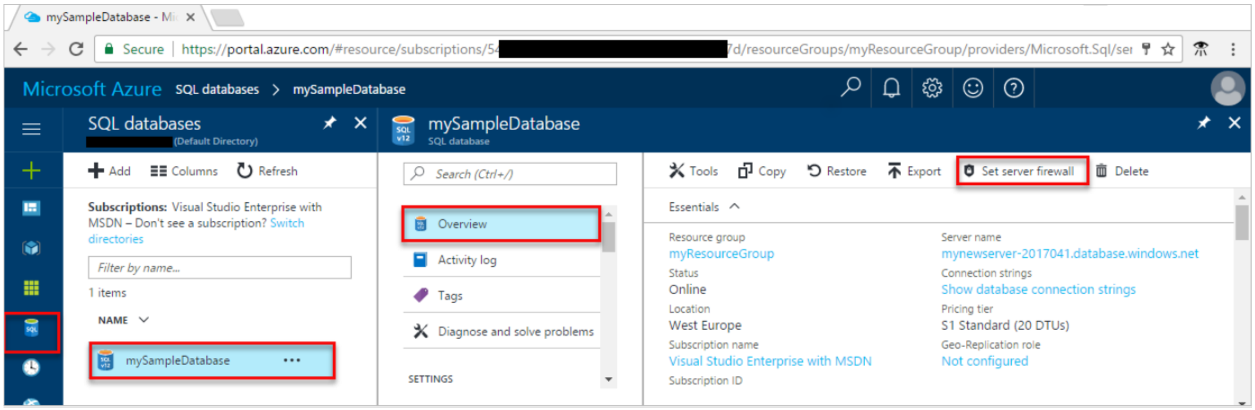
Use firewall rules to restrict database access

Microsoft Azure SQL Database provides a relational database service for Azure and other internet-based applications. To provide access security, SQL Database controls access with:

- Firewall rules that limit connectivity by IP address.
- Authentication mechanisms that require users to prove their identity.
- Authorization mechanisms that limit users to specific actions and data.

Firewalls prevent all access to your database server until you specify which computers have permission. The firewall grants access to databases based on the originating IP address of each request.

The following figure shows where you set a server firewall in SQL Database:


mySampleDatabase - Mi ×
Secure | https://portal.azure.com/#resource/subscriptions/5[redacted]7d/resourceGroups/myResourceGroup/providers/Microsoft.Sql/ser
Microsoft Azure SQL databases > mySampleDatabase
SQL databases
[redacted] (Default Directory)
Add Columns Refresh
Filter by name...
NAME
mySampleDatabase
mySampleDatabase
SQL database
Search (Ctrl+/)
Overview
Activity log
Tags
Diagnose and solve problems
SETTINGS
Tools Copy Restore Export Set server firewall Delete
Essentials

Subscriptions: Visual Studio Enterprise with MSDN – Don't see a subscription? Switch directories

1 items

Resource group: myResourceGroup
Status: Online
Location: West Europe
Subscription name: Visual Studio Enterprise with MSDN
Subscription ID
Server name: mynewserver-2017041.database.windows.net
Connection strings: Show database connection strings
Pricing tier: S1 Standard (20 DTUs)
Geo-Replication role: Not configured

The Azure SQL Database service is available only through TCP port 1433. To access a SQL database from your computer, ensure that your client computer firewall allows outgoing TCP communication on TCP port 1433. Block inbound connections on TCP port 1433 by using firewall rules, if you don't need these connections for other applications.

As part of the connection process, connections from Azure virtual machines are redirected to an IP address and port that are unique for each worker role. The port number is in the range from 11000 to 11999. For more information about TCP ports, see Ports beyond 1433 for ADO.NET 4.5.

For more information about firewall rules in SQL Database, see SQL Database firewall rules.

Note: In addition to IP rules, the firewall manages virtual network rules. Virtual network rules are based on virtual network service endpoints. Virtual network rules might be preferable to IP rules in some cases. To learn more, see Virtual network service endpoints and rules for Azure SQL Database.

Enable database authentication

SQL Database supports two types of authentication, SQL Server authentication and Azure AD authentication.

SQL Server authentication

Benefits of SQL Server authentication:

- It allows SQL Database to support environments with mixed operating systems, where all users are not authenticated by a Windows domain.
- Allows SQL Database to support older applications and partner-supplied applications that require SQL Server authentication.
- Allows users to connect from unknown or untrusted domains. An example is an application where established customers connect with assigned SQL Server logins to receive the status of their orders.
- Allows SQL Database to support web-based applications where users create their own identities.
- Allows software developers to distribute their applications by using a complex permission hierarchy based on known, preset SQL Server logins.

Note: SQL Server authentication cannot use the Kerberos security protocol.

If you use SQL Server authentication, you must:

- Manage the strong credentials yourself.
- Protect the credentials in the connection string.
- (Potentially) protect the credentials passed over the network from the web server to the database. For more information, see How to: Connect to SQL Server Using SQL Authentication in ASP.NET 2.0.

Azure AD authentication

Azure AD authentication is a mechanism of connecting to Azure SQL Database and SQL Data Warehouse by using identities in Azure AD. With Azure AD authentication, you can manage the identities of database users and other Microsoft services in one central location. Central ID management provides a single place to manage database users and simplifies permission management.

Note: We recommend the use of Azure AD authentication over the use of SQL Server authentication.

Benefits include the following:

- It provides an alternative to SQL Server authentication.
- It helps stop the proliferation of user identities across database servers.
- It allows password rotation in a single place.
- Customers can manage database permissions by using external (Azure AD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- It uses contained database users to authenticate identities at the database level.
- It supports token-based authentication for applications that connect to SQL Database.
- It supports AD FS (domain federation) or native user/password authentication for a local Azure Active Directory instance without domain synchronization.
- Azure AD supports connections from SQL Server Management Studio that use Active Directory Universal Authentication, which includes Multi-Factor Authentication. Multi-Factor Authentication provides strong authentication with a range of verification options—phone call, text message, smart cards with PIN, or mobile app notification. For more information, see SSMS support for Azure AD Multi-Factor Authentication with SQL Database and SQL Data Warehouse.

The configuration steps include the following procedures to configure and use Azure AD authentication:

- Create and populate Azure AD.
- Optional: Associate or change the Active Directory instance that's currently associated with your Azure subscription.
- Create an Azure Active Directory administrator for Azure SQL Database or Azure SQL Data Warehouse.
- Configure your client computers.
- Create contained database users in your database mapped to Azure AD identities.
- Connect to your database by using Azure AD identities.

You can find detailed information in Use Azure Active Directory authentication for authentication with SQL Database, Managed Instance, or SQL Data Warehouse.

Protect your data by using encryption

Azure SQL Database transparent data encryption helps protect data on disk and protects against unauthorized access to hardware. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. Transparent data encryption encrypts the storage of an entire database by using a symmetric key called the database encryption key.

Even when the entire storage is encrypted, it's important to also encrypt the database itself. This is an implementation of the defense-in-depth approach for data protection. If you're using Azure SQL Database and want to protect sensitive data (such as credit card or social security numbers), you can encrypt databases with FIPS 140-2 validated 256-bit AES encryption. This encryption meets the requirements of many industry standards (for example, HIPAA and PCI).

Files related to buffer pool extension (BPE) are not encrypted when you encrypt a database by using transparent data encryption. You must use file-system-level encryption tools like BitLocker or the Encrypting File System (EFS) for BPE-related files.

Because an authorized user like a security administrator or a database administrator can access the data even if the database is encrypted with transparent data encryption, you should also follow these recommendations:

- Enable SQL Server authentication at the database level.
- Use Azure AD authentication by using RBAC roles.
- Make sure that users and applications use separate accounts to authenticate. This way, you can limit the permissions granted to users and applications and reduce the risk of malicious activity.
- Implement database-level security by using fixed database roles (such as db_datareader or db_datawriter). Or you can create custom roles for your application to grant explicit permissions to selected database objects.

For other ways to encrypt your data, consider:

- Cell-level encryption to encrypt specific columns or even cells of data with different encryption keys.
- Always Encrypted, which allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine (SQL Database or SQL Server). As a result, Always Encrypted provides a separation between those who own the data (and can view it) and those who manage the data (but should have no access).
- Row-Level Security, which enables customers to control access to rows in a database table based on the characteristics of the user who is executing a query. (Example characteristics are group membership and execution context.)

Organizations that are not using database-level encryption might be more susceptible to attacks that compromise data located in SQL databases.

You can learn more about SQL Database transparent data encryption by reading the article Transparent Data Encryption with Azure SQL Database.

Enable database auditing

Auditing an instance of the SQL Server Database Engine or an individual database involves tracking and logging events. For SQL Server, you can create audits that contain specifications for server-level events and specifications for database-level events. Audited events can be written to the event logs or to audit files.

There are several levels of auditing for SQL Server, depending on government or standards requirements for your installation. SQL Server auditing provides tools and processes for enabling, storing, and viewing audits on various server and database objects.

Azure SQL Database auditing tracks database events and writes them to an audit log in your Azure storage account.

Auditing can help you maintain regulatory compliance, understand database activity, and find discrepancies and anomalies that might point to business concerns or security violations. Auditing facilitates adherence to compliance standards but doesn't guarantee compliance.

To learn more about database auditing and how to enable it, see Get started with SQL database auditing.

Enable database threat protection

Threat protection goes beyond detection. Database threat protection includes:

- Discovering and classifying your most sensitive data so you can protect your data.
- Implementing secure configurations on your database so you can protect your database.
- Detecting and responding to potential threats as they occur so you can quickly respond and remediate.

Best practices for database threat protection include:

Best practice	**Solution**
Discover, classify, and label the sensitive data in your databases.	Classify the data in your SQL database by enabling Data Discovery and Classification in Azure SQL Database. You can monitor access to your sensitive data in the Azure dashboard or download reports.
Track database vulnerabilities so you can proactively improve your database security.	Use the Azure SQL Database Vulnerability Assessment service, which scans for potential database vulnerabilities. The service employs a knowledge base of rules that flag security vulnerabilities and show deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data. The rules are based on Microsoft best practices and focus on the security issues that present the biggest risks to your database and its valuable data. They

Best practice	Solution
	cover both database-level issues and server-level security issues, like server firewall settings and server-level permissions. These rules also represent many of the requirements from regulatory bodies to meet their compliance standards.
Enable threat detection.	Enable Azure SQL Database Threat Detection to get security alerts and recommendations on how to investigate and mitigate threats. You get alerts about suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access and query patterns.

Advanced Threat Protection is a unified package for advanced SQL security capabilities. It includes the services mentioned earlier: Data Discovery and Classification, Vulnerability Assessment, and Threat Detection. It provides a single location for enabling and managing these capabilities.

Enabling these capabilities helps you:

- Meet data privacy standards and regulatory compliance requirements.
- Control access to your databases and harden their security.
- Monitor a dynamic database environment where changes are hard to track.
- Detect and respond to potential threats.

In addition, Threat Detection integrates alerts with Azure Security Center for a central view of the security state of all of your Azure resources.

Define and deploy strong operational security practices

Azure operational security refers to the services, controls, and features available to users for protecting their data, applications, and other assets in Azure. Azure operational security is built on a framework that incorporates the knowledge gained through capabilities that are unique to Microsoft, including the Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape.

The following sections describe best practices for operational security.

Manage and monitor user passwords

The following table lists some best practices related to managing user passwords:

Best practice	Solution
Ensure you have the proper level of password protection in the cloud.	Follow the guidance in Microsoft Password Guidance, which is scoped to users of the Microsoft identity

Best practice	Solution
	platforms (Azure Active Directory, Active Directory, and Microsoft account).
Monitor for suspicious actions related to your user accounts.	Monitor for users at risk and risky sign-ins by using Azure AD security reports.
Automatically detect and remediate high-risk passwords.	Azure AD Identity Protection is a feature of the Azure AD Premium P2 edition that enables you to: • Detect potential vulnerabilities that affect your organization's identities • Configure automated responses to detected suspicious actions that are related to your organization's identities • Investigate suspicious incidents and take appropriate actions to resolve them

Receive incident notifications from Microsoft

Be sure your security operations team receives Azure incident notifications from Microsoft. An incident notification lets your security team know you have compromised Azure resources so they can quickly respond to and remediate potential security risks.

In the Azure enrollment portal, you can ensure admin contact information includes details that notify security operations. Contact information is an email address and phone number.

Organize Azure subscriptions into management groups

If your organization has many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope that's above subscriptions. You organize subscriptions into containers called *management groups* and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group.

You can build a flexible structure of management groups and subscriptions into a directory. Each directory is given a single top-level management group called the *root* management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. The root management group allows global policies and RBAC assignments to be applied at the directory level.

Here are some best practices for using management groups:

Best practice	Solution
Ensure that new subscriptions apply governance elements like policies and permissions as they are added.	Use the root management group to assign enterprise-wide security elements that apply to all Azure assets. Policies and permissions are examples of elements.
Align the top levels of management groups with segmentation strategy to provide a point for control and policy consistency within each segment.	Create a single management group for each segment under the root management group. Don’t create any other management groups under the root.
Limit management group depth to avoid confusion that hampers both operations and security.	Limit your hierarchy to three levels, including the root.
Carefully select which items to apply to the entire enterprise with the root management group.	Ensure root management group elements have a clear need to be applied across every resource and that they’re low impact. Good candidates include: • Regulatory requirements that have a clear business impact (for example, restrictions related to data sovereignty) • Requirements with near-zero potential negative affect on operations, like policy with audit effect or RBAC permission assignments that have been carefully reviewed
Carefully plan and test all enterprise-wide changes on the root management group before applying them (policy, RBAC model, and so on).	Changes in the root management group can affect every resource on Azure. While they provide a powerful way to ensure consistency across the enterprise, errors or incorrect usage can negatively affect production operations. Test all changes to the root management group in a test lab or production pilot.

Streamline environment creation with blueprints

The Azure Blueprints service enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with a set of built-in components and the confidence that they're creating those environments within organizational compliance.

© 2018, Microsoft Corporation

Monitor storage services for unexpected changes in behavior

Diagnosing and troubleshooting issues in a distributed application hosted in a cloud environment can be more complex than it is in traditional environments. Applications can be deployed in a PaaS or IaaS infrastructure, on-premises, on a mobile device, or in some combination of these environments. Your application's network traffic might traverse public and private networks, and your application might use multiple storage technologies.

You should continuously monitor the storage services that your application uses for any unexpected changes in behavior (such as slower response times). Use logging to collect more detailed data and to analyze a problem in depth. The diagnostics information that you obtain from both monitoring and logging helps you to determine the root cause of the issue that your application encountered. Then you can troubleshoot the issue and determine the appropriate steps to remediate it.

Azure Storage Analytics performs logging and provides metrics data for an Azure storage account. We recommend that you use this data to trace requests, analyze usage trends, and diagnose issues with your storage account.

Prevent, detect, and respond to threats

Azure Security Center helps you prevent, detect, and respond to threats by providing increased visibility into (and control over) the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with various security solutions.

The Free tier of Security Center offers limited security for only your Azure resources. The Standard tier extends these capabilities to on-premises and other clouds. Security Center Standard helps you find and fix security vulnerabilities, apply access and application controls to block malicious activity, detect threats by using analytics and intelligence, and respond quickly when under attack. You can try Security Center Standard at no cost for the first 60 days. We recommend that you upgrade your Azure subscription to Security Center Standard.

Use Security Center to get a central view of the security state of all your Azure resources. At a glance, verify that the appropriate security controls are in place and configured correctly, and quickly identify any resources that need attention.

Security Center also integrates with Windows Defender Advanced Threat Protection (ATP), which provides comprehensive Endpoint Detection and Response (EDR) capabilities. With Windows Defender ATP integration, you can spot abnormalities. You can also detect and respond to advanced attacks on server endpoints monitored by Security Center.

Almost all enterprise organizations have a security information and event management (SIEM) system to help identify emerging threats by consolidating log information from diverse signal gathering devices. The logs are then analyzed by a data analytics system to help identify what’s “interesting” from the noise that is inevitable in all log gathering and analytics solutions.

Azure Sentinel is a scalable, cloud-native *security information and event management (SIEM)* and *security orchestration automated response (SOAR)* solution. Azure Sentinel provides intelligent security analytics and threat intelligence via alert detection, threat visibility, proactive hunting, and automated threat response.

Here are some best practices for preventing, detecting, and responding to threats:

Best practice	**Solution**
Increase the speed and scalability of your SIEM solution by using a cloud-based SIEM.	Investigate the features and capabilities of Azure Sentinel and compare them with the capabilities of what you're currently using on-premises. Consider adopting Azure Sentinel if it meets your organization's SIEM requirements.
Find the most serious security vulnerabilities so you can prioritize investigation.	Review your Azure secure score to see the recommendations resulting from the Azure policies and initiatives built into Azure Security Center. These recommendations help address top risks like security updates, endpoint protection, encryption, security configurations, missing WAF, internet-connected VMs, and many more. The secure score, which is based on Center for Internet Security (CIS) controls, lets you benchmark your organization's Azure security against external sources. External validation helps validate and enrich your team's security strategy.
Monitor the security posture of machines, networks, storage and data services, and applications to discover and prioritize potential security issues.	Follow the security recommendations in Security Center starting, with the highest priority items.
Integrate Security Center alerts into your security information and event management (SIEM) solution.	Most organizations with a SIEM use it as a central clearinghouse for security alerts that require an analyst response. Processed events produced by Security Center are published to the Azure Activity Log, one of the logs available through Azure Monitor. Azure Monitor offers a consolidated pipeline for routing any of your monitoring data into a SIEM tool. See Integrate security solutions in Security Center for instructions. If you're using Azure Sentinel, see Connect Azure Security Center.
Integrate Azure logs with your SIEM.	Use Azure Monitor to gather and export data. This practice is critical for enabling security incident investigation, and online log retention is limited. If you're using Azure Sentinel, see Connect data sources.
Speed up your investigation and hunting processes and reduce false positives by integrating Endpoint	Enable Windows Defender ATP integration via your Security Center security policy. Consider using Azure Sentinel for threat hunting and incident response.

Detection and Response (EDR) capabilities into your attack investigation.	

Monitor end-to-end scenario-based network monitoring

Customers build an end-to-end network in Azure by combining network resources like a virtual network, ExpressRoute, Application Gateway, and load balancers. Monitoring is available on each of the network resources.

Azure Network Watcher is a regional service. Use its diagnostic and visualization tools to monitor and diagnose conditions at a network scenario level in, to, and from Azure.

The following table lists best practices for network monitoring and available tools:

Best practice	**Solution**
Automate remote network monitoring with packet capture.	Monitor and diagnose networking issues without logging in to your VMs by using Network Watcher. Trigger packet capture by setting alerts and gain access to real-time performance information at the packet level. When you see an issue, you can investigate in detail for better diagnoses.
Gain insight into your network traffic by using flow logs.	Build a deeper understanding of your network traffic patterns by using network security group flow logs. Information in flow logs helps you gather data for compliance, auditing, and monitoring your network security profile.
Diagnose VPN connectivity issues.	Use Network Watcher to diagnose your most common VPN Gateway and connection issues. You can not only identify the issue but also use detailed logs to further investigate.

Secure deployment by using proven DevOps tools

Use the following DevOps best practices to ensure that your enterprise and teams are productive and efficient:

Best practice	**Solution**
Automate the build and deployment of services.	Infrastructure as code is a set of techniques and practices that help IT pros remove the burden of day-to-day build and management of modular infrastructure. It enables IT pros to build and maintain their modern server

Best practice	Solution
	environment in a way that's like how software developers build and maintain application code. You can use Azure Resource Manager to provision your applications by using a declarative template. In a single template, you can deploy multiple services along with their dependencies. You use the same template to repeatedly deploy your application in every stage of the application lifecycle.
Automatically build and deploy to Azure web apps or cloud services.	You can configure your Azure DevOps projects to automatically build and deploy to Azure web apps or cloud services. Azure DevOps automatically deploys the binaries after doing a build to Azure after every code check-in. The package build process is equivalent to the Package command in Visual Studio, and the publishing steps are equivalent to the Publish command in Visual Studio.
Automate release management.	Azure Pipelines is a solution for automating multiple-stage deployment and managing the release process. Create managed continuous deployment pipelines to release quickly, easily, and often. With Azure Pipelines, you can automate your release process, and you can have predefined approval workflows. Deploy on-premises and to the cloud, extend, and customize as required.
Check your app's performance before you launch it or deploy updates to production.	Run cloud-based load tests to: • Find performance problems in your app. • Improve deployment quality. • Make sure that your app is always available. • Make sure that your app can handle traffic for your next launch or marketing campaign. Apache JMeter is a free, popular open source tool with a strong community backing.
Monitor application performance.	Azure Application Insights is an extensible application performance management (APM) service for web developers on multiple platforms. Use Application Insights to monitor your live web application. It automatically detects performance anomalies. It includes analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability.

Mitigate and protect against DDoS

Distributed denial of service (DDoS) is a type of attack that tries to exhaust application resources. The goal is to affect the application's availability and its ability to handle legitimate requests. These attacks are becoming more sophisticated and larger in size and impact. They can be targeted at any endpoint that is publicly reachable through the internet.

Designing and building for DDoS resiliency requires planning and designing for a variety of failure modes. The following table lists best practices for building DDoS-resilient services on Azure:

Best practice	Solution
Ensure that security is a priority throughout the entire lifecycle of an application, from design and implementation to deployment and operations. Applications can have bugs that allow a relatively low volume of requests to use a lot of resources, resulting in a service outage.	To help protect a service running on Microsoft Azure, you should have a good understanding of your application architecture and focus on the five pillars of software quality. You should know typical traffic volumes, the connectivity model between the application and other applications, and the service endpoints that are exposed to the public internet. Ensuring that an application is resilient enough to handle a denial of service that's targeted at the application itself is most important. Security and privacy are built into the Azure platform, beginning with the Security Development Lifecycle. The SDL addresses security at every development phase and ensures that Azure is continually updated to make it even more secure.
Design your applications to scale horizontally to meet the demand of an amplified load, specifically in the event of a DDoS attack. If your application depends on a single instance of a service, it creates a single point of failure. Provisioning multiple instances makes your system more resilient and more scalable.	For Azure App Service, select an App Service plan that offers multiple instances. For Azure Cloud Services, configure each of your roles to use multiple instances. For Azure Virtual Machines, ensure that your VM architecture includes more than one VM and that each VM is included in an availability set. We recommend using virtual machine scale sets for autoscaling capabilities.
Layering security defenses in an application reduces the chance of a successful attack. Implement secure designs for your applications by using the built-in capabilities of the Azure platform.	The risk of attack increases with the size (surface area) of the application. You can reduce the surface area by using whitelisting to close down the exposed IP address space and listening ports that are not needed on the load balancers (Azure Load Balancer and Azure Application Gateway). Network security groups are another way to reduce the attack surface. You can use service tags and application security

Best practice	Solution
	groups to minimize complexity for creating security rules and configuring network security, as a natural extension of an application's structure. You should deploy Azure services in a virtual network whenever possible. This practice allows service resources to communicate through private IP addresses. Azure service traffic from a virtual network uses public IP addresses as source IP addresses by default. Using service endpoints switches service traffic to use virtual network private addresses as the source IP addresses when they're accessing the Azure service from a virtual network. We often see customers' on-premises resources getting attacked along with their resources in Azure. If you're connecting an on-premises environment to Azure, minimize exposure of on-premises resources to the public internet.

Azure has two DDoS service offerings that provide protection from network attacks:

- Basic protection is integrated into Azure by default at no additional cost. The scale and capacity of the globally deployed Azure network provides defense against common network-layer attacks through always-on traffic monitoring and real-time mitigation. Basic requires no user configuration or application changes and helps protect all Azure services, including PaaS services like Azure DNS.
- Standard protection provides advanced DDoS mitigation capabilities against network attacks. It's automatically tuned to protect your specific Azure resources. Protection is simple to enable during the creation of virtual networks. It can also be done after creation and requires no application or resource changes.

Enable Azure Policy

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies.

Enable Azure Policy to monitor and enforce your organization's written policy. This will ensure compliance with your company or regulatory security requirements by centrally managing security policies across your hybrid cloud workloads. Learn how to create and manage policies to enforce compliance. See Azure Policy definition structure for an overview of the elements of a policy.

Here are some security best practices to follow after you adopt Azure Policy:

Best practice	Solution
Policy supports several types of effects. You can read about them in Azure Policy definition structure. Business operations can be negatively affected by the **deny** effect and the **remediate** effect, so start with the **audit** effect to limit the risk of negative impact from policy.	Start policy deployments in **audit** mode and then later progress to **deny** or **remediate**. Test and review the results of the **audit** effect before you move to **deny** or **remediate**. For more information, see Create and manage policies to enforce compliance.
Identify the roles responsible for monitoring for policy violations and ensuring the right remediation action is taken quickly.	Have the assigned role monitor compliance through the Azure portal or via the command line.
Azure Policy is a technical representation of an organization's written policies. Map all Azure policies to organizational policies to reduce confusion and increase consistency.	Document mapping in your organization's documentation or in the Azure policy itself by adding a reference to the organizational policy in the Azure policy description or the Azure policy initiative description.

Monitor Azure AD risk reports

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. Discovering compromised identities is no easy task. Azure AD uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user accounts. Each detected suspicious action is stored in a record called a risk event. Risk events recorded in Azure AD security reports. For more information, read about the users at risk security report and the risky sign-ins security report.

Design, build, and manage secure cloud applications

An application that uses the most advanced security measures can still be undone by simple design errors. A security feature doesn't need to be compromised if it can be avoided. This is just as true for applications in the cloud as it is for conventional deployments.

Using platform-based (PaaS) services can offer tremendous value to an organization by shifting some responsibilities to the provider. Organizations can improve their threat detection and response times by using a provider's cloud-based security capabilities and cloud intelligence. By shifting responsibilities to the cloud provider, organizations can get more security coverage, which enables them to move security resources and budget to other business priorities.

Although Azure is responsible for securing the underlying infrastructure and platform, it's your responsibility to develop, deploy, and manage your application in a secure way. Otherwise, your application code is vulnerable to threats like SQL injection, session hijacking, and cross-site scripting.

The following sections describe security best practices for cloud applications.

Adopt a policy of identity as the primary security perimeter

When you're designing and managing cloud applications, it's important to change your focus from a network-centric approach to an identity-centric approach to perimeter security. With PaaS deployments, you shift from needing to control everything yourself to sharing responsibility with Microsoft.

The following table lists best practices for managing the identity perimeter:

Best practice	**Solution**
Secure your keys and credentials to secure your PaaS deployment.	Losing keys and credentials is a common problem. You can use a centralized solution where keys and secrets can be stored in hardware security modules. Azure provides you an HSM in the cloud with Azure Key Vault.
Don't put credentials and other secrets in source code or GitHub.	The only thing worse than losing your keys and credentials is having an unauthorized party gain access to them. Attackers can take advantage of bot technologies to find keys and secrets stored in code repositories such as GitHub. Do not put key and secrets in these public code repositories.
Protect your VM management interfaces on hybrid PaaS and IaaS services by using a management interface that enables you to remote manage these VMs directly.	Remote management protocols such as SSH, RDP, and PowerShell remoting can be used. In general, we recommend that you do not enable direct remote access to VMs from the internet. If possible, use alternate approaches like using virtual private networks in an Azure virtual network. If alternative approaches are not available, ensure that you use complex passphrases and two-factor authentication (such as Azure Multi-Factor Authentication).
Use strong authentication and authorization platforms.	Use federated identities in Azure AD instead of custom user stores. When you use federated identities, you take advantage of a platform-based approach and you delegate the management of authorized identities to your partners. A federated identity approach is especially important when employees are terminated and that information needs to be reflected through multiple identity and authorization systems. Use platform-supplied authentication and authorization mechanisms instead of custom code. The reason is that developing custom authentication code can be error prone. Most of your developers are not security experts and are

Best practice	Solution
	unlikely to be aware of the subtleties and the latest developments in authentication and authorization. Commercial code (for example, from Microsoft) is often extensively security reviewed. Use two-factor authentication. Two-factor authentication is the current standard for authentication and authorization because it avoids the security weaknesses inherent in username and password types of authentication. Access to both the Azure management (portal/remote PowerShell) interfaces and customer-facing services should be designed and configured to use Azure Multi-Factor Authentication. Use standard authentication protocols, such as OAuth2 and Kerberos. These protocols have been extensively peer reviewed and are likely implemented as part of your platform libraries for authentication and authorization.

Use threat modeling during application design

The Microsoft Security Development Lifecycle specifies that teams should engage in a process called threat modeling during the design phase. To help facilitate this process, Microsoft has created the SDL Threat Modeling Tool. Modeling the application design and enumerating STRIDE threats across all trust boundaries can catch design errors early on.

The following table lists the STRIDE threats and gives some example mitigations that use Azure features. These mitigations won't work in every situation.

Threat	Security property	Potential Azure platform mitigation
Spoofing	Authentication	Require HTTPS connections.
Tampering	Integrity	Validate SSL certificates.
Repudiation	Non-repudiation	Enable Azure monitoring and diagnostics.
Information disclosure	Confidentiality	Encrypt sensitive data at rest by using service certificates.
Denial of service	Availability	Monitor performance metrics for potential denial-of-service conditions. Implement connection filters.

Threat	Security property	Potential Azure platform mitigation
Elevation of privilege	Authorization	Use Privileged Identity Management.

Develop on Azure App Service

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

Best practices for using App Service are:

Best practice	Solution
Authenticate through Azure Active Directory.	App Service provides an OAuth 2.0 service for your identity provider. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, and mobile phones. Azure AD uses OAuth 2.0 to enable you to authorize access to mobile and web applications.
Restrict access based on the need to know and least privilege security principles.	Restricting access is imperative for organizations that want to enforce security policies for data access. You can use RBAC to assign permissions to users, groups, and applications at a certain scope.
Protect your keys.	Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use. With Key Vault, you can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs. See Azure Key Vault to learn more. You can also use Key Vault to manage your TLS certificates with auto-renewal.
Restrict incoming source IP addresses.	App Service Environment has a virtual network integration feature that helps you restrict incoming source IP addresses through network security groups. Virtual networks enable you to

© 2018, Microsoft Corporation

Best practice	Solution
	place Azure resources in a non-internet, routable network that you control access to. To learn more, see Integrate your app with an Azure virtual network.
Monitor the security state of your App Service environments.	Use Azure Security Center to monitor your App Service environments. When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls. **Note:** Monitoring App Service is in preview and available only on the Standard tier of Security Center.

Install a web application firewall

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

Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities. WAF is based on rules from the OWASP (Open Web Application Security Project) core rule sets 3.0 or 2.2.9.

Monitor the performance of your applications

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

Use Azure Application Insights to monitor availability, performance, and usage of your application, whether it's hosted in the cloud or on-premises. By using Application Insights, you can quickly identify and diagnose errors in your application without waiting for a user to report them. With the information that you collect, you can make informed choices on your application's maintenance and improvements.

Application Insights has extensive tools for interacting with the data that it collects. Application Insights stores its data in a common repository. It can take advantage of shared functionality such as alerts, dashboards, and deep analysis with the Log Analytics query language.

Perform security penetration testing

Validating security defenses is as important as testing any other functionality. Make penetration testing a standard part of your build and deployment process. Schedule regular security tests and vulnerability scanning on deployed applications, and monitor for open ports, endpoints, and attacks.

Fuzz testing is a method for finding program failures (code errors) by supplying malformed input data to program interfaces (entry points) that parse and consume this data. Microsoft Security Risk Detection is a cloud-based tool that you can use to look for bugs and other security vulnerabilities in your software before you deploy it to Azure. The tool is designed to catch vulnerabilities before you deploy software so you don't have to patch a bug, deal with crashes, or respond to an attack after the software is released.

Next steps

For more information about Azure security, see the in-depth security topics on the Azure Security Documentation website.

For more information on security best practices, see Azure security best practices and patterns.

Find blog posts about Azure security and compliance on the Azure security blog.

Resources

The following resources address specialized services that might apply to your unique environment and elevate your security capabilities:

- What is Azure Dedicated HSM?
    - Identify whether you need to use dedicated hardware security modules (HSMs) to meet regulatory or security requirements.
    - Identify whether you need to import or generate keys in HSMs that never leave the HSM boundary to meet regulatory or security requirements.
- Azure confidential computing. Identify whether you need to use confidential computing to meet regulatory or security requirements.

Use the following resources to learn more about Azure and the best practices and services discussed in this paper:

- Shared Responsibilities for Cloud Computing: Understand the division of responsibility between you and Microsoft in a SaaS, PaaS, and IaaS deployment.
- Azure enterprise scaffold - prescriptive subscription governance: Get guidance on first steps to take after you decide to move to Azure.

- Choose the right authentication method for your Azure Active Directory hybrid identity solution: Learn how to implement a complete Azure AD hybrid identity solution, focusing on the right authentication method.
- How to successfully roll out self-service password reset: Learn more about deploying password reset and training users to use it.
- What is role-based access control?: Learn more about RBAC and how it works.
- What is Azure Policy?: Understand how Azure Policy is different from RBAC and how to create policies with Azure Resource Manager.
- Get started with Azure Key Vault: Learn how to set up a key vault by using PowerShell.
- Azure Disk Encryption for Windows and Linux IaaS VMs: Learn more about Azure Disk Encryption, including prerequisites and deployment scenarios.
- Securing privileged access: Learn more about securing privileged access and privileged access workstations.
- Securing your SQL database: Understand the basics of securing the data tier of an application by using Azure SQL Database.
- Monitor a storage account in the Azure portal: Learn how to enable logging and configure metrics and in Storage Analytics.
- Monitor, diagnose, and troubleshoot Microsoft Azure Storage: Learn how to use Storage Analytics and other tools to identify, diagnose, and troubleshoot Azure Storage.
- Configure Network Watcher: Learn how to configure and enable Network Watcher.
- Azure operational security: Understand Microsoft's approach to Azure operational security within the Azure platform.
- PaaS deployments: Learn more about securing PaaS deployments.
- Azure Service Fabric security best practices: Before deploying a cloud application into production, review recommended best practices for implementing secure clusters in the application.