

- [Microsoft Azure Well-Architected Framework - 安全性](#)

# 简介

- 2 分钟

安全性是任何体系结构最为重视的方面之一。确保业务数据和客户数据安全是非常重要的。公共数据泄露可能会破坏公司的声誉，并给个人造成重大损害和财务损失。

在过去，安全只专注于通过强大的外围防御来抵御恶意的黑客攻击。这种机制防御外围之外的事物，而在“墙”内，组织系统受到信任。而现在的安全状况是假定漏洞并采用“零信任模型”。

安全专业人员不再侧重于外围防御。在数据和服务访问方面，现代组织必须对企业防火墙以内和以外都提供平等的支持。

在这里，你将了解 Azure 架构良好的框架的安全性支柱。

本模块中讨论的概念未包含所有内容，但介绍了在云中生成解决方案的一些重要注意事项。有关 Azure Well-Architected Framework 的更多详细信息，请在开始规划和设计体系结构时访问 [Azure 体系结构中心](#)。

## 学习目标

学完本模块后，你将能够：

- 开发深层防御方法来保护体系结构的安全
- 选择用于保护 Azure 基础结构的技术
- 制定安全标识管理策略

## 先决条件

- 拥有使用核心基础结构技术（例如数据存储、计算和网络）生成或操作解决方案的经验
- 拥有通过生成或操作技术系统来解决业务问题的经验

## 深层防御

- 10 分钟

从安全性角度来看，不存在可解决所有问题的简单解决方案。让我们假设一下，你在一家组织工作，该组织之前忽视了它环境的安全性。该公司已意识到需要重点关注这一领域。但不确定从何处着手，也不知道是否只需购买解决方案就可确保其环境安全。公司只知道需要一个整体方法，但又不确定什么方法才适合。

在这里，我们将明确深层防御的主要概念，并确定支持深层防御策略的关键安全技术和方法。我们还将讨论在构建自己的 Azure 服务时如何应用这些概念。

## 零信任模型

分析公司 Forrester Research 引入了“零信任模型”，意在永远不应假定信任，而是应该不断验证信任。当用户、设备和数据都留在组织的防火墙中时，它们被假定为受信任。这种假定的信任允许在恶意黑客盗用终结点设备后轻松地进行横向移动。

现在，大多数用户都可以通过 Internet 访问应用程序和数据，而许多公司现在允许用户在工作中使用自己的设备（自带设备办公或称 BYOD）。事务的大多数组成部分（用户、网络和设备）不再完全受组织控制。零信任模型依赖于可验证的用户和设备信任声明来授予对组织资源的访问权限。不再因为其位于组织外围以内就假定信任。

该模型迫使安全研究人员、工程师和架构师重新考虑应用于安全性的方法，并使用分层策略来保护其资源。

## 深层防御：安全分层方法

深层防御策略采用一系列机制减缓攻击进展，这些攻击旨在获取对信息的未经授权访问。每层都可提供保护，以便在某层出现安全漏洞后，后续层能就位以防止进一步泄露。

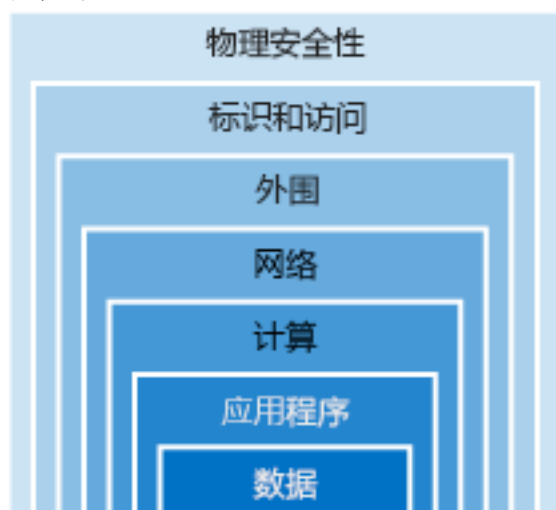
Microsoft 同时在物理数据中心和整个 Azure 服务中应用分层安全方法。深层防御的目的是保护信息，防止信息被未经授权访问的人员窃取。有助于定义安全状态的通用原则是机密性、完整性和可用性，统称为 CIA。

- 保密性：最小特权原则将对信息的访问限制为仅显式授予访问权限的个人。该信息包括对用户密码、远程访问证书和电子邮件内容的保护。
- 完整性：目的是防止对静态或传输中的信息进行未经授权的更改。发送方在数据传输中使用的常见方法是使用单向哈希算法创建唯一的数据指纹。哈希与数据一起发送给接收方。接收方重新计算数据哈希并与原始数据相比，以确保数据未在传输过程中丢失或修改。
- 可用性：确保授权用户可使用服务。拒绝服务攻击是导致用户可用性下降的常见原因。自然灾害同样推动了系统设计，以防止单一故障点，并将应用程序的多个实例部署到地理分散的位置。

## 安全层

可以将深层防御形象化为一组同心圆环，将要保护的数据放在中心。每个环在数据周围都增设了一层安全保护。这种方法消除了对任何单个保护层的依赖。它还可以降低攻击速度并提供可以自动或手动执行的警报遥测。

我们来了解一下这些层。



每层都可以实现一个或多个 CIA 关注点：

安全层

#	环	示例	原则
1	数据	Azure Blob 存储中的静态数据加密	完整性
2	应用程序	SSL/TLS 加密会话	完整性
3	计算	OS 和分层软件修补程序的常规应用程序	可用性
4	网络	网络安全规则	保密性
5	外围	DDoS 防护	可用性
6	身份验证和访问控制	Azure Active Directory 用户身份验证	完整性
7	物理安全性	Azure 数据中心生物识别访问控制	机密性

## 数据

在几乎所有情况下，攻击者都会攻击以下数据：

- 存储在数据库中的数据。
- 存储在虚拟机内的磁盘上的数据。
- 存储在软件即服务 (SaaS) 应用程序中，例如 Microsoft 365。
- 存储在云存储中。

存储和控制对数据的访问的人员有责任确保数据的安全。通常情况下，相应法规要求规定必须提供数据控制和处理方式，确保数据的保密性、完整性和可用性。

## 应用程序

- 确保应用程序安全且没有任何漏洞。
- 将敏感的应用程序机密存储在安全的存储介质中。
- 将安全性包含在所有应用程序开发的设计要求中。

将安全性融合到应用程序开发生命周期，有助于减少代码中出现的安全漏洞数量。鼓励所有开发团队在默认情况下确保其应用程序处于安全状态。必须不打折扣地执行安全性要求。

## 计算

- 对虚拟机的安全访问。
- 实现终结点保护，修复系统并使其保持最新。

恶意软件、未修复的系统和保护不当的系统将使环境容易受到攻击。此层的重点是确保计算资源安全，同时设置适当的控制以最大程度减少安全问题。

## 网络

- 通过分段和访问控制限制资源之间的通信。
- 默认拒绝。
- 限制入站 Internet 访问并在适当的时候限制出站访问。
- 实现与本地网络的安全连接。

此层的重点是限制所有资源之间的网络连接。将资源细分，利用网络级别的控制限制只能与所需的内容进行通信。通过限制该通信，可降低整个网络中发生横向位移的风险。

## 外围

- 使用分布式拒绝服务 (DDoS) 防护来筛选大规模攻击，以免用户遭受拒绝服务攻击。
- 使用外围防火墙可识别针对网络的恶意攻击，并发出警报。

在网络外围，其职责是防止针对资源的基于网络的攻击。识别这些攻击、消除其影响并在攻击发生时发出警报，这对于保持网络安全至关重要。

## 身份验证和访问控制

- 控制对基础结构的访问（变更控制）。
- 使用单一登录和多重身份验证。
- 审核事件和更改。

标识和访问层的职责是确保标识安全、所授予访问权限仅为所需权限以及记录更改。













## 物理安全性

以物理方式构建安全性和控制对数据中心内计算硬件的访问是第一道防线。

利用物理安全性，可针对资产访问提供物理安全保护。这可确保不能绕过其他层，进而恰当处理丢失或盗取问题。

## 共担责任

随着计算环境从客户控制的数据中心转移到云数据中心，安全责任也将转移。现在安全性是云提供商和客户共同面对的问题。

责任	本地	IaaS	PaaS	SaaS
数据管理和权限管理				
客户端终结点				
帐户和访问管理				
标识和目录基础结构				
应用程序				
网络控制				
操作系统				
物理主机				
物理网络				
物理数据中心				

 Microsoft
 客户

## 持续改进

威胁形势正大规模实时演变，因此安全体系结构没有绝对的完善。Microsoft 及其客户需要能够以智能的方式，快速地大规模响应这些威胁。

Azure 安全中心为客户提供统一的安全管理和高级威胁防护，以理解和响应本地和 Azure 中的安全事件。反过来，Azure 客户有责任不断地对其安全体系结构进行再评估和改进。

## 知识检测

1. 判断正误：深层防御是一种策略，旨在防范尝试获取信息访问权限的攻击。

正确

错误

2. 判断正误：通过迁移到云，可确保体系结构完全安全，并且可将所有安全责任移交给云提供商。

正确

错误

检查你的答案

**D  
e  
f  
e  
n  
s  
e  
i  
n  
d  
e  
p**

# t h

- 10 minutes

There's no easy solution that solves all your problems from a security perspective. Let's imagine you work for an organization that has neglected security in its environment. The company has realized that it needs to put some major focus in this area. The company isn't sure where to start, or if it's possible to just buy a solution to make the environment secure. The company knows it needs a holistic approach but is unsure what fits into that.

Here, we'll identify key concepts of defense in depth and identify key security technologies and approaches to support a defense-in-depth strategy. We'll also discuss how to apply these concepts when you're architecting your own Azure services.

## Zero Trust model

The analyst firm Forrester Research introduced the *Zero Trust model*, which states that you should never assume trust but instead continually validate trust. When users, devices, and data all resided inside the organization's firewall, they were assumed to be trusted. This assumed trust allowed for easy lateral movement after a malicious hacker compromised an endpoint device. Most users now access applications and data from the internet, and many companies now allow users to use their own devices at work (*bring your own device*, or BYOD). Most components of the transactions--the users, network, and devices--are no longer completely under organizational control. The Zero Trust model relies on verifiable user and device trust claims to grant access to organizational resources. No longer is trust assumed based on the location inside an organization's perimeter.

This model has forced security researchers, engineers, and architects to rethink the approach applied to security and use a layered strategy to protect their resources.

## Defense in depth: A layered approach to security

*Defense in depth* is a strategy that employs a series of mechanisms to slow the advance of an attack that's aimed at acquiring unauthorized access to information. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure.

Microsoft applies a layered approach to security, both in its physical datacenters and across Azure services. The objective of defense in depth is to protect information and prevent it from being stolen by individuals who aren't authorized to access it. The common principles that help define a security posture are confidentiality, integrity, and availability, known collectively as CIA.

- **Confidentiality:** The principle of least privilege restricts access to information only to individuals explicitly granted access. This information includes protection of user



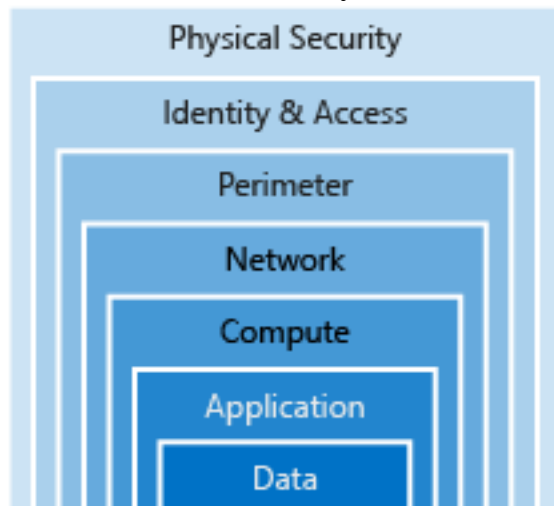
passwords, remote access certificates, and email content.

- **Integrity:** The goal is to prevent unauthorized changes to information at rest or in transit. A common approach used in data transmission is for the sender to create a unique fingerprint of the data by using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The receiver recalculates the data's hash and compares it to the original to ensure that the data wasn't lost or modified in transit.
- **Availability:** Ensure that services are available to authorized users. Denial-of-service attacks are a common cause of loss of availability to users. Natural disasters also drive system design to prevent single points of failure and deploy multiple instances of an application to geo-dispersed locations.

## Security layers

You can visualize defense in depth as a set of concentric rings, with the data to be secured at the center. Each ring adds a layer of security around the data. This approach removes reliance on any single layer of protection. It also acts to slow down an attack and provide alert telemetry that can be acted upon, either automatically or manually.

Let's look at each of the layers.



Each layer can implement one or more of the CIA concerns:

SECURITY LAYERS			
#	Ring	Example	Principle
1	Data	Data encryption at rest in Azure Blob Storage	Integrity
2	Application	SSL/TLS encrypted sessions	Integrity

3	Compute	Regular application of OS and layered software patches	Availability
4	Network	Network security rules	Confidentiality
5	Perimeter	DDoS protection	Availability
6	Identity and access	Azure Active Directory user authentication	Integrity
7	Physical security	Azure datacenter biometric access controls	Confidentiality

## Data

In almost all cases, attackers are after data:

- Stored in a database.
- Stored on disk inside virtual machines.
- Stored on a software as a service (SaaS) application such as Microsoft 365.
- Stored in cloud storage.

The people who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

## Applications

- Ensure that applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.

Integrating security into the application development life cycle will help reduce the number of vulnerabilities introduced in code. Encourage all development teams to make their applications secure by default. Make security requirements non-negotiable.

## Compute

- Secure access to virtual machines.
- Implement endpoint protection and keep systems patched and current.

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure, and that you have the proper controls in place to minimize security issues.

# Networking

- Limit communication between resources through segmentation and access controls.
- Deny by default.
- Restrict inbound internet access and limit outbound where appropriate.
- Implement secure connectivity to on-premises networks.

At this layer, the focus is on limiting network connectivity across all your resources. Segment your resources and use network-level controls to restrict communication to only what's needed. By limiting this communication, you reduce the risk of lateral movement throughout your network.

## Perimeter

- Use distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting on them are important to keep your network secure.

## Identity and access

- Control access to infrastructure (change control).
- Use single sign-on and multifactor authentication.
- Audit events and changes.

The identity and access layer is all about ensuring that identities are secure, access granted is only what's needed, and changes are logged.









































## Physical security



Physical building security and controlling access to computing hardware within the datacenter are the first line of defense.

With physical security, the intent is to provide physical safeguards against access to assets. This ensures that other layers can't be bypassed, and that loss or theft is handled appropriately.

## Shared responsibilities

As computing environments move from customer-controlled datacenters to cloud datacenters, the responsibility of security also shifts. Security is now a concern that both cloud providers and customers share.

Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management				
Client endpoints				
Account & access management				
Identity & directory infrastructure				
Application				
Network controls				
Operating system				
Physical hosts				
Physical network				
Physical datacenter				

 Microsoft
  Customer

## Continuous improvement

The threat landscape is evolving in real time and at massive scale, so a security architecture is never complete. Microsoft and its customers need the ability to respond to these threats intelligently, quickly, and at scale.

Azure Security Center provides customers with unified security management and advanced threat protection to understand and respond to security events on-premises and in Azure. In turn, Azure customers have a responsibility to continually reevaluate and evolve their security architecture.

## Check your knowledge

1. True or false: *defense in depth* is a strategy aimed to protect you against attacks that try to gain access to your information.

True

False

2. True or false: by moving to the cloud, your architecture is fully secure and you can hand off all security responsibilities to your cloud provider.

True

False

Check your answers

# 标识管理

- 10 分钟

假设你在一个医疗保健组织中工作，该组织运行内部应用程序和 Web 门户，使其临床医生可以在其中管理患者健康数据。该组织已收到向护理人员提供此应用程序的诸多请求，这些护理人员通常与患者待在一起，因此不在使用网络的人员范围内。

最近，由于恶意代理导致数据泄漏，迫使公司增强其密码策略。该公司现在要求用户更频繁地更改其密码，并使用更长、更复杂的密码。这导致出现了不必要的负面影响，由于难以记住为不同管理角色创建的多组凭证，用户便以不安全的方式记录复杂密码。在这里，我们将介绍作为内部和外部应用程序安全层的标识。我们还将介绍单一登录 (SSO) 和多重身份验证提供标识安全性的好

处，以及为何要考虑将本地标识复制到 Azure Active Directory (Azure AD)。

## 作为安全层的标识

数字标识是当今本地和联机业务和社交互动不可缺少的一部分。过去，标识和访问服务仅限于在公司的内部网络中运行。

Kerberos 和 LDAP 等协议旨在实现此目的。

最近，移动设备已成为人们与数字服务进行交互的主要方式。客户和员工都希望能够随时随地访问服务。这种期望推动了标识协议的发展，这些协议可以在许多不同的设备和操作系统上通过 Internet 运行。

当你的组织评估其体系结构在标识方面的功能时，正在研究如何将以下功能融入应用程序：

- 为应用程序用户提供单一登录功能。
- 增强应用程序，以轻松使用新式身份验证。
- 对公司网络之外的所有登录实施多重身份验证。
- 开发应用程序，允许患者注册并安全地管理其帐户数据。

## 单一登录

用户需要管理的标识越多，凭证相关的安全事故风险就越大。更多的标识意味着需要记住和更改更多的密码。密码策略可能因应用程序而异。随着复杂性要求增加，用户更加难以记住这些密码。

另一方面是所有这些标识所需的管理。支持人员处理帐户锁定和密码重置请求时，将会承受更多的压力。如果用户离开组织，追踪所有这些标识并确保它们已被禁用会非常困难。被忽略的标识可以允许进行应被消除的访问。

使用单一登录，用户只需记住一个 ID 和一个密码。跨应用程序的访问权限将授予给绑定到用户的单个标识，从而简化了安全模型。当用户更改角色或离开组织时，访问权限修改仅与单个标识相关联，大大减少了更改或禁用帐户所需的工作量。对帐户使用单一登录，用户可以更轻松地管理其标识。它还将增强环境中的安全功能。

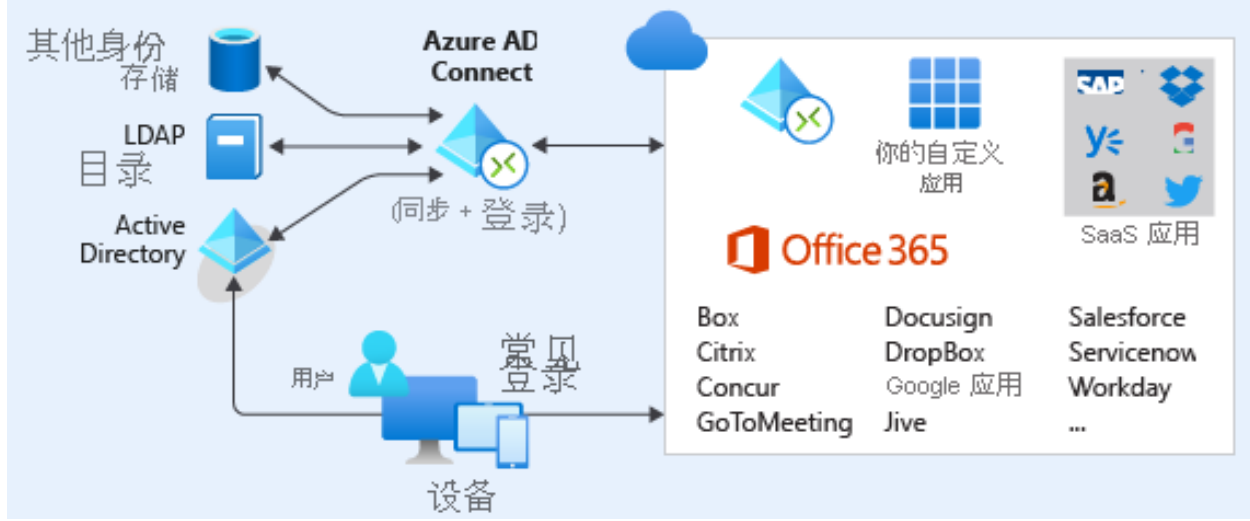
## **Azure Active Directory 的 SSO**

Azure AD 是一种基于云的标识服务。它具有内置支持，可与本地 Active Directory 实例同步，也可单独使用。这意味着所有应用程序无论是在本地、云中（包括 Microsoft 365）还是在移动设备中，都可共享相同的凭证。管理员和开发人员可以使用 Azure AD 中配置的集中式规则和策略来控制对数据和应用程序的访问。通过将 Azure AD 用于 SSO，你还可以将多个数据源组合成一个智能安全图。此安全图可以帮助你为 Azure AD 中的所有帐户（包括从本地 Active Directory 同步的帐户）提供威胁分析和实时标识保护。通过使用集中式标识提供程序，你可以将标识基础结构的安全控制、报告、警报和管理集中起来。

## **将目录与 Azure AD Connect 同步**

Azure AD Connect 可将本地目录与 Azure Active Directory 集成。Azure AD Connect 提供最新功能，并替换旧版标识集成工具（例如 DirSync 和 Azure AD Sync）。单个工具即可提供轻松同步和登录的部署体验。

## Azure AD Connect:你的身份桥



你的组织要求主要针对本地域控制器进行身份验证，但还需要在灾难恢复方案中进行云身份验证。Azure AD 满足组织的所有要求。你的组织已决定继续进行以下配置：

- 使用 Azure AD Connect 将存储于本地 Active Directory 中的组、用户帐户和密码哈希同步到 Azure AD。在传递身份验证不可用的情况下，这可作为备用选项。
- 使用 Windows Server 上安装的本地身份验证代理配置传递身份验证。
- 使用 Azure AD 的无缝 SSO 登录功能从本地已加入域的电脑中自动让用户登录。SSO 通过禁止多个身份验证请求减少用户冲突。

## 身份验证和访问权限

你的组织的安全策略要求发生在公司外围网络之外的所有登录都使用附加的一重身份验证进行身份验证。此要求将 Azure AD 服务的两个方面（即多重身份验证和条件访问策略）相结合。



# 多重身份验证

多重身份验证通过要求使用两个及以上的元素进行完全身份验证，为标识提供额外的安全性。这些元素分为三个类别：

- 已知内容：密码或安全性问题的答案。
- 已有内容：接收通知的移动应用或令牌生成设备。
- 自身特性：某种生物识别属性，例如在许多移动设备上使用的指纹或面部扫描。

使用多重身份验证可通过限制凭证暴露的影响来提高标识的安全性。如果攻击者拥有用户的密码，还需要使用他们的手机或脸部才能完全进行身份验证。仅进行单一因素身份验证并不足够，攻击者无法使用上述凭证进行身份验证。这给安全性带来的好处是巨大的，因此组织应尽量启用多重身份验证。

Azure AD 具有内置的多重身份验证功能，并将与其他多重身份验证提供程序集成。Microsoft 365 和 Azure AD 管理员可免费使用基本多重身份验证功能。如果要升级管理员的功能，或将多重身份验证扩展给其余用户，可以购买更多的功能。

## 条件访问策略

除多重身份验证外，还需先确保已满足其他要求，授予访问权限才能增加另一层保护。阻止来自可疑 IP 地址的登录，或拒绝来自无恶意软件保护的设备的访问，可限制风险登录的访问。

Azure Active Directory 提供基于组、位置或设备状态的条件访问策略。位置功能使你的组织能够区分不属于其网络的 IP 地址，并满足其安全策略，要求来自所有此类位置的访问进行多重身份验证。你的组织创建了条件访问策略，要求从公司网络外的 IP 地址访问应用程序的用户面临使用多重身份验证的挑战。

在下图中，首先根据条件列表检查访问本地和云应用程序的用户请求。请求会被允许访问、强制执行多重身份验证，或根据它们满足的条件被阻止。



## 保护应用程序

你的员工需要安全地远程访问其在本地上托管的管理应用程序。目前，用户在企业防火墙后使用 Windows 集成身份验证从其加入域的计算机向应用程序进行身份验证。

尽管已制定将新式身份验证机制融合到应用程序的项目计划，但尽快实现远程访问功能仍存在相当大的业务压力。Azure AD 应用程序代理可让用户在不更改任何代码的情况下远程访问应用程序。

Azure AD 应用程序代理的特性：

- 简单
  - 无需更改或更新应用程序即可使用应用程序代理。
  - 用户可获得一致的身份验证体验。他们可以使用 MyApps 门户单一登录到云中的 SaaS 应用和本地应用。
- 安全
  - 使用 Azure AD 应用程序代理发布应用时，可利用 Azure 中的授权控件和安全分析功能。可以获得云级安全性和 Azure 安全功能，例如条件访问和双重验证。

- 无需通过防火墙打开任何入站连接即可让用户进行远程访问。
- 经济高效
- 应用程序代理在云中运行，因此可以节省时间和资金。本地解决方案通常需要设置和维护外围网络、边缘服务器或其他复杂的基础结构。

Azure AD 应用程序代理有两个组件。一个是位于公司网络中运行 Windows 的服务器上的连接器代理，另一个是外部终结点（MyApps 门户或外部 URL）。用户转到终结点时，使用 Azure AD 进行身份验证并通过连接器代理路由到本地应用程序。

## 处理使用者标识

将新式身份验证与其现有应用程序集成在一起后，组织很快便认识到了托管标识系统（例如 Azure AD）的好处。现在，领导团队想要探索利用 Microsoft 标识服务增加业务价值的其他方式。该团队将注意力集中在外部客户上，并关注现有客户交互方式的现代化如何提供与标识提供者（如 Google、Facebook 和 LinkedIn）的紧密集成。

Azure AD B2C 是以 Azure Active Directory 为基础而构建的身份管理服务。通过该服务，可以自定义和控制客户在使用应用程序时注册、登录和管理其个人资料的方式。此类应用程序包括为 iOS、Android、.NET 等系统开发的应用程序。

Azure AD B2C 可提供社交标识登录体验，同时保护客户标识个人资料信息。Azure AD B2C 目录不同于标准的 Azure AD 目录，并且可以在 Azure 门户中创建。

## 知识检测

1. 以下哪项不是单一登录的优势？

增加用户权限分配的复杂性

减少用户需要记住的 ID 和密码数量

减少用户更改角色或离开组织时的管理工作量

确保在各个应用程序间采用一致的密码策略

2. 与密码结合使用时，以下哪一项是对多重身份验证有效的第二个元素？

驾驶证

基于时间的一次性密码

帐号

卡密钥

**I  
d  
e  
n  
ti  
t  
y  
m  
a  
n**

# agente ment

- 10 minutes

Imagine you work for a healthcare organization that hosts an internal application and web portal for its clinicians to manage patient health data. The organization has received many requests for this application to be available to caregivers, who are often on-site with patients and therefore outside the network.

A recent data leak by malicious agents has forced the company to tighten its password policies. The company now requires users to change their passwords more frequently and use longer, more complex passwords. This has led to the unwanted side effect of users recording complex passwords insecurely as they struggle to remember multiple sets of credentials created for different administrative roles.

Here, we'll discuss identity as a security layer for internal and external applications. We'll also discuss the benefits of single sign-on (SSO) and multifactor authentication to provide identity security, and why to consider replicating on-premises identities to Azure Active Directory (Azure AD).

## Identity as a layer of security

Digital identities are an integral part of today's business and social interactions on-premises and online. In the past, identity and access services were restricted to operating within a company's internal network. Protocols such as Kerberos and LDAP were designed for this purpose.

More recently, mobile devices have become the primary way that people interact with digital services. Customers and employees alike expect to be able to access services from anywhere at any time. This expectation has driven the development of identity protocols that can work at internet scale across many disparate devices and operating systems.

As your organization evaluates the capabilities of its architecture around identity, it's looking at ways to bring the following capabilities into the application:

- Provide single-sign on to application users.
- Enhance the application to use modern authentication with minimal effort.

- Enforce multifactor authentication for all sign-ins outside the company's network.
- Develop an application to allow patients to enroll and securely manage their account data.

## **Single sign-on**

The more identities a user has to manage, the greater the risk of a credential-related security incident. More identities mean more passwords to remember and change. Password policies can vary between applications. As complexity requirements increase, it's more difficult for users to remember them.

On the other side is the management required for all those identities. Additional strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring that they're disabled can be challenging. An overlooked identity can allow access that should have been eliminated.

With single sign-on, users need to remember only one ID and one password. Access across applications is granted to a single identity tied to a user, simplifying the security model. As users change roles or leave an organization, access modifications are tied to the single identity, greatly reducing the effort needed to change or disable accounts.

Using single sign-on for accounts will make it easier for users to manage their identities. It will also increase the security capabilities in your environment.

## **SSO with Azure Active Directory**

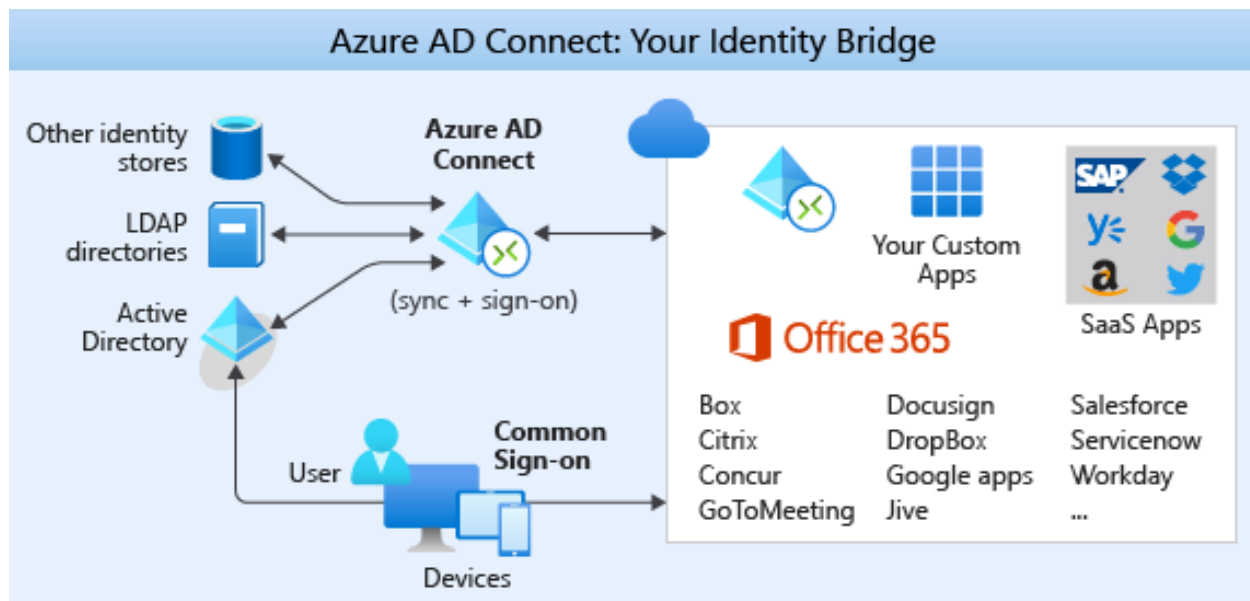
Azure AD is a cloud-based identity service. It has built-in support for synchronizing with your on-premises Active Directory instance, or it can be used on its own. This means that all your applications, whether on-premises, in the cloud (including Microsoft 365), or even mobile, can share the same credentials. Administrators and developers can control access to data and applications by using centralized rules and policies configured in Azure AD.

By using Azure AD for SSO, you'll also have the ability to combine multiple data sources into an intelligent security graph. This security graph can help you provide threat analysis and real-time identity protection to all accounts in Azure AD, including accounts that are synchronized from on-premises Active Directory. By using a centralized identity provider, you'll have centralized the security controls, reporting, alerting, and administration of your identity infrastructure.

## **Synchronize directories with Azure AD Connect**

Azure AD Connect can integrate your on-premises directories with Azure Active Directory. Azure AD Connect provides the newest capabilities and replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

It's a single tool to provide an easy deployment experience for synchronization and sign-in.



Your organization requires that authentication occurs primarily against on-premises domain controllers, but it also requires cloud authentication in a disaster recovery scenario. It doesn't have any requirements that Azure AD doesn't already support.

Your organization has made the decision to move forward with the following configuration:

- Use Azure AD Connect to synchronize groups, user accounts, and password hashes stored in on-premises Active Directory to Azure AD.  
This can be a backup if pass-through authentication is unavailable.
- Configure pass-through authentication by using an on-premises authentication agent installed on Windows Server.
- Use the seamless SSO feature of Azure AD to automatically sign in users from on-premises domain-joined computers.  
SSO reduces user friction by suppressing multiple authentication requests.

## Authentication and access

Your organization's security policy requires that all sign-ins that occur outside the company's perimeter network are authenticated with an additional factor of authentication. This requirement combines two aspects of the Azure AD service: multifactor authentication and conditional access policies.

### Multifactor authentication

Multifactor authentication provides additional security for your identities by requiring two or more elements for full authentication. These elements fall into three categories:

- *Something you know*: A password or the answer to a security question.

- *Something you have*: A mobile app that receives a notification or a token-generating device.
- *Something you are*: Some sort of biometric property such as a fingerprint or face scan used on many mobile devices.

Using multifactor authentication increases the security of your identity by limiting the impact of credential exposure. An attacker who has a user's password would also need to have possession of their phone or their face in order to fully authenticate. Authentication with only a single factor verified is insufficient, and the attacker would be unable to use those credentials to authenticate. The benefits that this brings to security are huge, so organizations should enable multifactor authentication wherever possible.

Azure AD has multifactor authentication capabilities built in and will integrate with other multifactor authentication providers. Basic multifactor authentication features are available to Microsoft 365 and Azure AD administrators for no extra cost. If you want to upgrade the features for your admins or extend multifactor authentication to the rest of your users, you can purchase more capabilities.

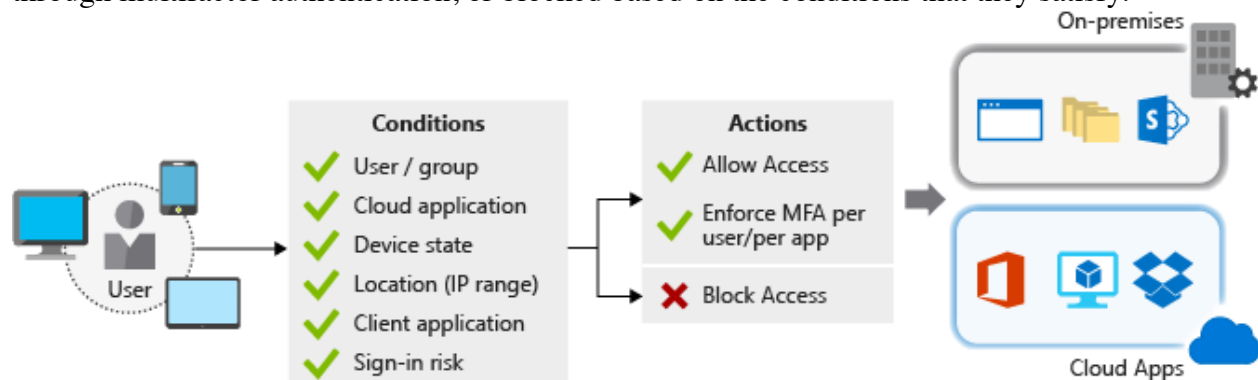
## Conditional access policies

Along with multifactor authentication, ensuring that additional requirements are met before granting access can add another layer of protection. Blocking logins from a suspicious IP address, or denying access from devices without malware protection, can limit access from risky sign-ins.

Azure Active Directory provides conditional access policies based on group, location, or device state. The location feature allows your organization to differentiate IP addresses that don't belong to the network, and it satisfies the security policy to require multifactor authentication from all such locations.

Your organization has created a conditional access policy that requires users who access the application from an IP address outside the company network to be challenged with multifactor authentication.

In the following illustration, user requests to access the on-premises and cloud applications are first checked against a list of conditions. The requests are either allowed access, forced to go through multifactor authentication, or blocked based on the conditions that they satisfy.



## Securing applications



Your employees require secure remote access to their administrative application hosted on-premises. Users currently authenticate to the application by using Windows Integrated Authentication from their domain-joined machines, behind the corporate firewall.

Although a project to incorporate modern authentication mechanisms into the application has been planned, there's considerable business pressure to enable remote access capabilities as soon as possible. Azure AD Application Proxy can allow users to access the application remotely without any code changes.

Azure AD Application Proxy is:

- Simple
  - You don't need to change or update your applications to work with Application Proxy.
  - Your users get a consistent authentication experience. They can use the MyApps portal to get single sign-on to both SaaS apps in the cloud and your apps on-premises.
- Secure
  - When you publish your apps by using Azure AD Application Proxy, you can take advantage of the authorization controls and security analytics in Azure. You get cloud-scale security and Azure security features like conditional access and two-step verification.
  - You don't have to open any inbound connections through your firewall to give your users remote access.
- Cost-effective
  - Application Proxy works in the cloud, so you can save time and money. On-premises solutions typically require you to set up and maintain perimeter networks, edge servers, or other complex infrastructures.

Azure AD Application Proxy has two components. The first is a connector agent that sits on a server running Windows within your corporate network. The second is an external endpoint, either the MyApps portal or an external URL. When a user goes to the endpoint, they authenticate with Azure AD and are routed to the on-premises application via the connector agent.

## Working with consumer identities

Since your organization integrated modern authentication with its existing application, it has quickly acknowledged the benefits of a managed identity system such as Azure AD. The leadership team is now interested in exploring other ways that Microsoft identity services can add business value. The team is focusing its attention on external customers and how modernization of existing customer interactions might provide tight integration with identity providers like Google, Facebook, and LinkedIn.

Azure AD B2C is an identity management service that's built on the foundation of Azure Active Directory. It enables you to customize and control how customers sign up, sign in, and manage their profiles when using your applications. This includes applications developed for iOS, Android, and .NET, among others.

Azure AD B2C provides a social identity login experience, while at the same time protecting your customer identity profile information. Azure AD B2C directories are distinct from standard Azure AD directories and can be created in the Azure portal.

# Check your knowledge

1. Which of the following is *not* a benefit of single sign-on?

Increased complexity in assigning permissions to users

Fewer IDs and passwords for users to remember

Lower administration effort when users change roles or leave an organization

Ensuring a consistent password policy across applications

2. Which of the following would be a valid second element for multifactor authentication, when combined with a password?

A driver's license

A time-based one-time password

Your account number

Your car keys

Check your answers

保  
护  
基  
础  
结  
构

- 10 分钟

假设你的组织最近经历了一次面向客户的 Web 应用程序的重大故障。某个工程师对包含生产 Web 应用程序的资源组具备完全访问权限。该工程师意外删除了资源组以及所有子资源，包括托管实时客户数据的数据库。

幸运的是，应用程序源代码和资源可在源代码管理工具中找到，并且按计划自动进行了定期数据库备份。对该服务的恢复工作会相对轻松一些。在这里，我们将探索组织如何使用 Azure 中的功能来保护对基础结构的访问，从而避免此中断。

## 基础结构的重要程度

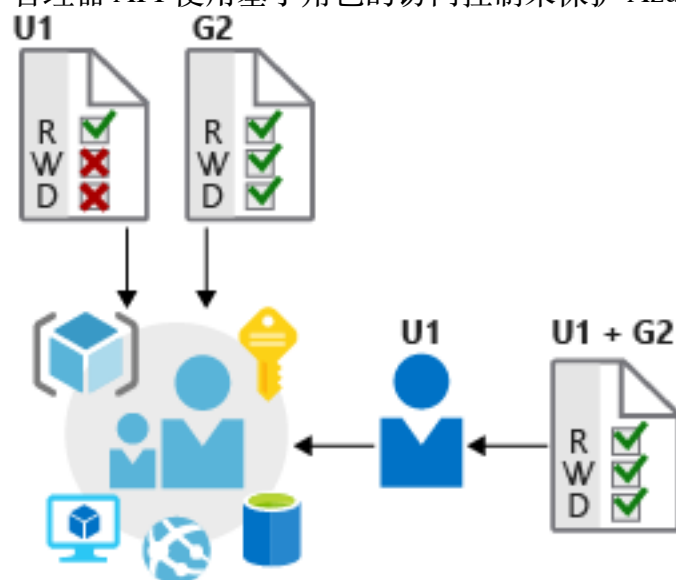
云基础结构逐渐成为许多企业不可或缺的部分。必须确保人员和进程仅具备完成作业所需的权限。如果权限分配不恰当，则会导致数据丢失、数据泄露或服务不可用。

系统管理员可能会对大量用户、系统和权限集负责。因此，很快他们就会难以准确管理授权，并导致使用“一刀切”方法。这种方法可以降低管理工作的复杂性，但是所授予的权限极有可能高于需要的权限。

## 基于角色的访问控制

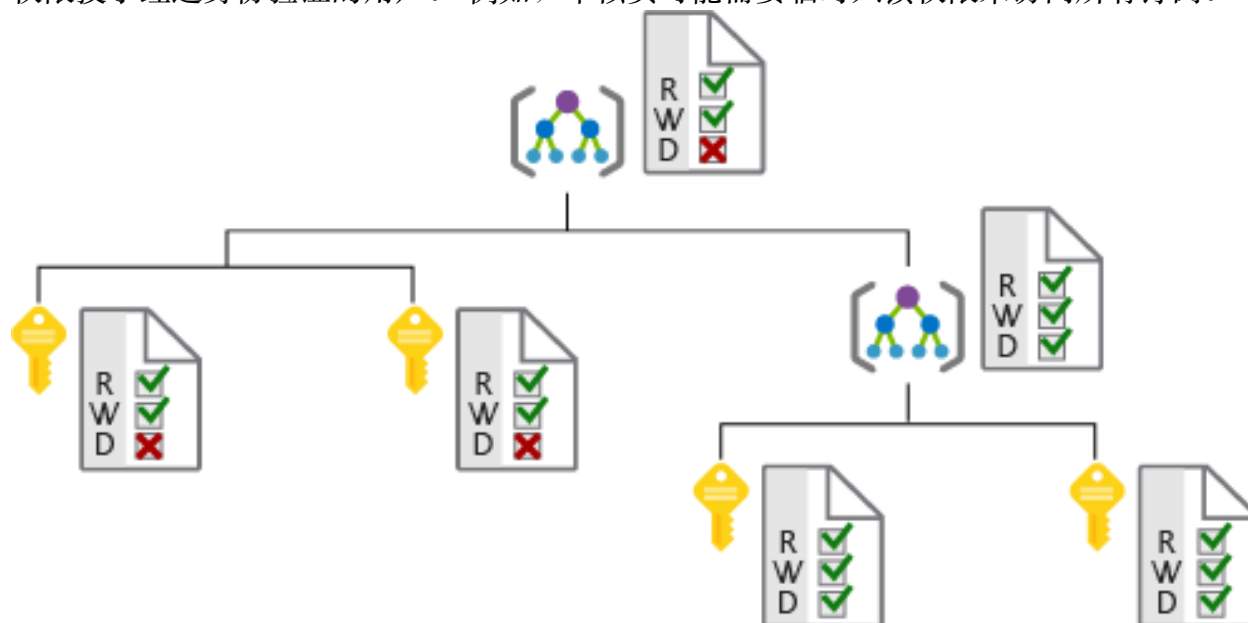
基于角色的访问控制 (RBAC) 提供了一种略有不同的方法。它将角色定义为访问权限的集合。将安全主体直接地或通过组成员身份间接地映射至角色。将安全主体、访问权限和资源分离，从而简化访问权限管理并提供更详细的控制。

在 Azure 上，用户、组 and 角色都存储在 Azure Active Directory (Azure AD) 中。Azure 资源管理器 API 使用基于角色的访问控制来保护 Azure 中所有资源的访问权限管理。



## 角色和管理组

角色是权限集（例如“只读”或“参与者”），用户可以获取角色以便访问 Azure 服务实例。可在单个服务实例级别授予角色，但角色也可沿 Azure 资源管理器层次结构向下传递。在更高的范围（例如整个订阅）分配的角色会由子范围（例如服务实例）继承。管理组是最近引入 RBAC 模型的另一个层次级别。管理组添加了对订阅进行分组归纳以及将策略应用于更高级别的功能。管理员也可借助通过任意定义的订阅层次结构传递角色的功能，将对整个环境的临时访问权限授予经过身份验证的用户。例如，审核员可能需要临时只读权限来访问所有订阅。



## Privileged Identity Management

除使用 RBAC 来管理 Azure 资源访问权限外，一个全面的基础设施保护方法还应考虑将角色成员的持续审核纳入其组织的变化和发展过程中。Azure AD Privileged Identity Management (PIM) 是一项额外的付费产品/服务，用于监督角色分配、自助服务和实时角色 (JIT) 激活。



使用 Azure AD PIM 服务，可以管理、控制和监视对组织中的重要资源的访问。这包括访问 Azure AD、Azure 和其他 Microsoft Online Services（如 Microsoft 365 或 Microsoft Intune）中的资源。在这样的控制下，用户还是需要在 Azure AD、Azure、Microsoft 365 和软件即服务 (SaaS) 应用中执行特权操作。

组织可能会授予用户对 Azure 资源和 Azure AD 的 JIT 特许访问权限。需要监督这些用户使用其管理特权执行了哪些操作。PIM 有助于缓解访问权限过度、不必要或滥用的风险。

下面是 PIM 的一些重要功能：

- 提供对 Azure AD 和 Azure 资源的实时特权访问权限
- 使用开始和结束日期分配对资源的限时访问权限
- 要求获得批准才能激活特权角色
- 强制执行 Azure AD 多重身份验证以激活任何角色
- 使用理由来了解用户激活角色的原因
- 激活特权角色时获取通知
- 开展访问评审，以确保用户仍然需要角色
- 下载审核历史记录来进行内部或外部审核

若要使用 PIM，需要拥有以下付费或试用许可证之一：

- Azure AD Premium P2
- 企业移动性 + 安全性 (EMS) E5

## 对服务提供标识

标识对服务来说通常是很有用的。通常，根据最佳做法，凭证信息嵌入在配置文件中。这些配置文件不具备任何安全性，任何能够访问系统或存储库的人员都可访问这些凭证，而这会带来信息暴露的风险。

Azure AD 通过两种方法来解决此问题：服务主体和 Azure 服务的托管标识。

## 服务主体

若要理解服务主体，最好先理解“标识”和“主体”这两个词，因为在身份管理领域中会用到它们。

“标识”只是一个可以进行身份验证的内容。很显然，它包括带有用户名和密码的用户，但还可以包括可能会使用密钥或证书进行身份验证的应用程序或其他服务器。“帐户”是一种额外的定义，指的是与标识关联的数据。

“主体”是充当特定角色或声明的标识。考虑在 Bash 提示符下或通过“以管理员身份运行”在 Windows 上使用 Sudo。在这两种情况下，你仍然可以使用之前的同一标识登录，只是角色不同而已。

因此，服务主体已按字面指定。它是服务或应用程序所使用的标识。可以如其他标识一样向其分配角色。

例如，你的组织可以将其部署脚本指定为以服务主体身份进行身份验证。如果这是唯一一个有权限执行破坏性操作的标识，你的组织就能在很大程度上确保不会再出现意外删除资源的情况。

## Azure 资源的托管标识

创建服务主体的过程可能比较繁琐。并且还有许多方面使得难以维护服务主体。Azure 资源的托管标识会简单很多，并可为你完成大部分的工作。

可以立即为任何支持托管标识的 Azure 服务创建此标识。（列表还在不断增加。）为服务创建托管标识时，会在 Azure AD 租户上创建一个帐户。Azure 基础结构会自动对该服务进行身份验证并管理该帐户。然后便可像使用其他任何 Active Directory 帐户一样使用该帐户，包括安全地使经过身份验证的服务访问其他 Azure 资源。

## 知识检查

1. Azure 基于角色的访问控制可以应用于除以下哪个作用域外的所有访问控制？

订阅

资源组

Linux 文件系统中的文件和文件夹

资源

2. 判断正误：可以将 Azure 资源的托管标识分配给某虚拟机，使其有权启动和停止其他虚拟机。

True

错误

检查你的答案

**I  
n  
f  
r  
a  
s  
t  
r  
u  
c  
t  
u  
r  
e**

# **p r o t e c t i o n**

- 10 minutes

Imagine your organization recently experienced a significant outage to a customer-facing web application. An engineer was granted full access to a resource group that contains the production web application. This engineer accidentally deleted the resource group and all child resources, including the database that hosts live customer data.

Fortunately, the application source code and resources were available in source control and regular database backups were running automatically on a schedule. The service was reinstated relatively easily. Here, we'll explore how the organization could have avoided this outage by using capabilities in Azure to protect access to the infrastructure.

## **Criticality of infrastructure**

Cloud infrastructure is becoming an essential piece of many businesses. It's critical to ensure that people and processes have only the rights they need to get their job done. Assigning incorrect access can result in data loss, data leakage, or unavailability of services.

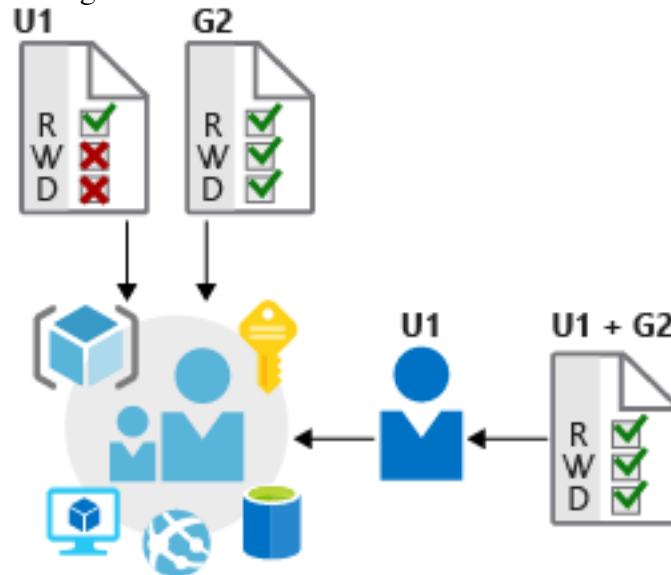
System administrators can be responsible for a large number of users, systems, and permission sets. So correctly granting access can quickly become unmanageable and can lead to a "one size fits all" approach. This approach can reduce the complexity of administration, but makes it far easier to inadvertently grant more permissive access than required.

## **Role-based access control**



Role-based access control (RBAC) offers a slightly different approach. Roles are defined as collections of access permissions. Security principals are mapped to roles directly or through group membership. Separating security principals, access permissions, and resources provides simplified access management and more detailed control.

On Azure, users, groups, and roles are all stored in Azure Active Directory (Azure AD). The Azure Resource Manager API uses role-based access control to secure all resource access management within Azure.

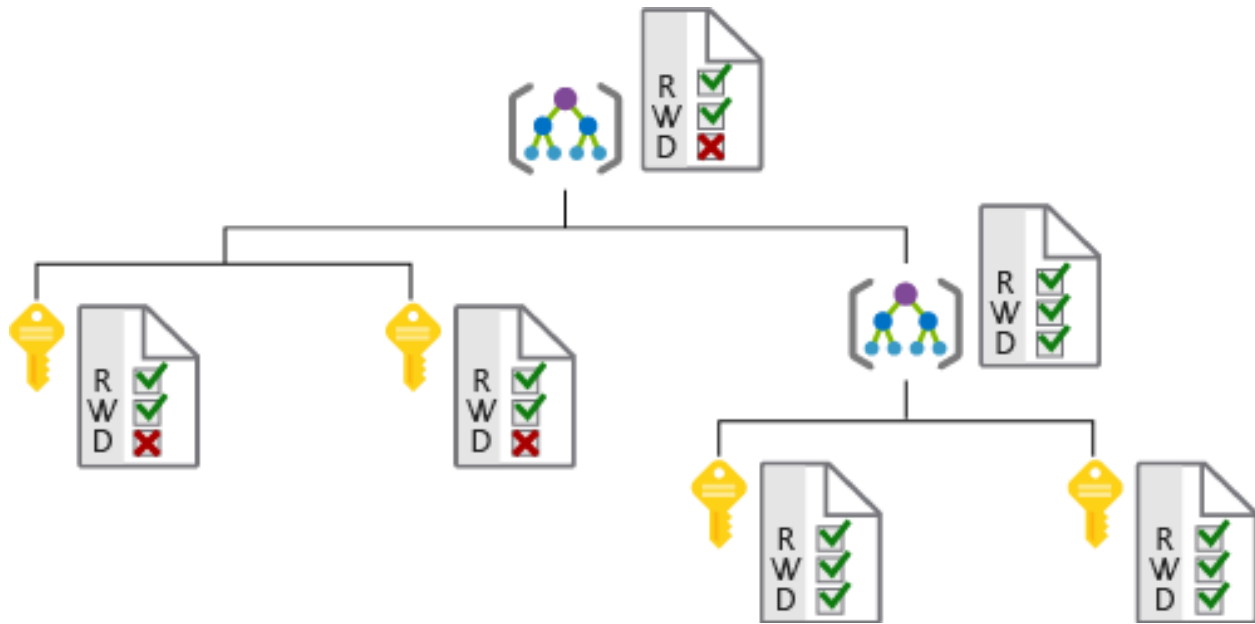


## Roles and management groups

Roles are sets of permissions, like *read-only* or *contributor*, that users can be granted to access an Azure service instance. Roles can be granted at the level of an individual service instance, but they also flow down the Azure Resource Manager hierarchy. Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.

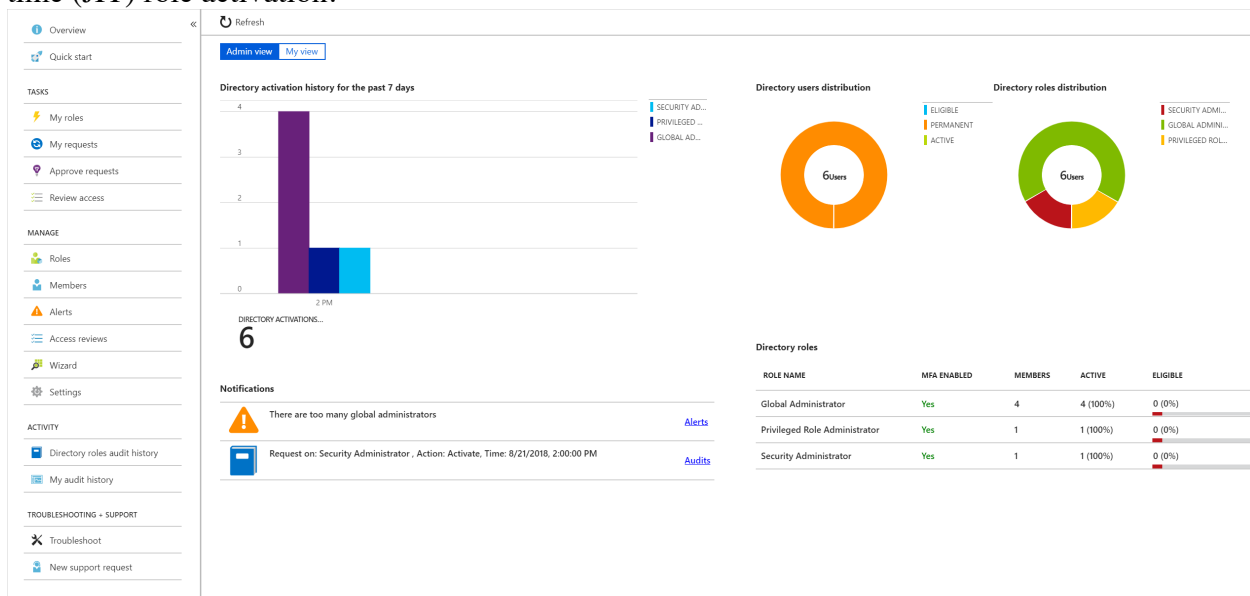
Management groups are an additional hierarchical level recently introduced into the RBAC model. Management groups add the ability to group subscriptions together and apply policy at an even higher level.

The ability to flow roles through an arbitrarily defined subscription hierarchy also allows administrators to grant temporary access to an entire environment for authenticated users. For example, an auditor might require temporary read-only access to all subscriptions.



## Privileged Identity Management

In addition to managing Azure resource access with RBAC, a comprehensive approach to infrastructure protection should consider including the ongoing auditing of role members as the organization changes and evolves. Azure AD Privileged Identity Management (PIM) is an additional paid-for offering that provides oversight of role assignments, self-service, and just-in-time (JIT) role activation.



With the Azure AD PIM service, you can manage, control, and monitor access to important resources in your organization. This includes access to resources in Azure AD; Azure; and other Microsoft Online Services, like Microsoft 365 and Microsoft Intune. This control does not eliminate the need for users to carry out privileged operations in Azure AD, Azure, Microsoft 365, and software as a service (SaaS) apps.

Organizations can give users JIT privileged access to Azure resources and Azure AD. Oversight is needed for what those users do with their administrator privileges. PIM helps mitigate the risk of excessive, unnecessary, or misused access rights.

Here are some of the key features of PIM:

- Providing just-in-time privileged access to Azure AD and Azure resources
- Assigning time-bound access to resources by using start and end dates
- Requiring approval to activate privileged roles
- Enforcing Azure AD multifactor authentication to activate any role
- Using justification to understand why users activate
- Getting notifications when privileged roles are activated
- Conducting access reviews to ensure that users still need roles
- Downloading an audit history for an internal or external audit

To use PIM, you need one of the following paid or trial licenses:

- Azure AD Premium P2
- Enterprise Mobility + Security (EMS) E5

## Providing identities to services

It's often valuable for services to have identities. Often, and against best practices, credential information is embedded in configuration files. With no security around these configuration files, anyone with access to the systems or repositories can access these credentials and risk exposure. Azure AD addresses this problem through two methods: service principals and managed identities for Azure services.

### Service principals

To understand service principals, it's useful to first understand the words *identity* and *principal* as they're used in the world of identity management.

An *identity* is just a thing that can be authenticated. Obviously, this includes users with usernames and passwords. But it can also include applications or other servers, which might authenticate with secret keys or certificates. As a bonus definition, an *account* is data associated with an identity.

A *principal* is an identity that acts with certain roles or claims. Consider the use of Sudo on a Bash prompt or on Windows via **Run as administrator**. In both of those cases, you're still signed in as the same identity as before, but you've changed your role.

So, a *service principal* is literally named. It's an identity that a service or application uses. Like other identities, it can be assigned roles.

For example, your organization can assign its deployment scripts to run authenticated as a service principal. If that's the only identity that has permission to perform destructive actions, your organization has gone a long way toward making sure that it doesn't repeat the accidental resource deletion.

### Managed identities for Azure resources

The creation of service principals can be a tedious process. There are also many touch points that can make maintaining service principals difficult. Managed identities for Azure resources are much easier and will do most of the work for you.

A managed identity can be instantly created for any Azure service that supports it. (The list is constantly growing.) When you create a managed identity for a service, you're creating an account on the Azure AD tenant. Azure infrastructure will automatically take care of authenticating the service and managing the account. You can then use that account like any other Active Directory account, including letting the authenticated service securely access other Azure resources.

## Check your knowledge

1. Azure role-based access control can be applied to all but which of the following scopes?

Subscription

Resource group

Files and folders within a Linux file system

Resource

2. True or false: a managed identity for Azure resources can be assigned to a virtual machine to give it rights to start and stop other virtual machines.

True

False

Check your answers

## 加密

- 10 分钟

数据是组织最宝贵且不可替代的资产。加密是数据分层安全策略中的最后一道也是最坚固的防线。

假设你在一个医疗保健组织中工作，它存储了大量敏感数据。该组织最近遇到了数据泄露事件，该事件公开了患者未加密的敏感数据。该组织现已充分意识到其数据保护功能存在漏洞。它想了解如何更好地使用加密来保护自己 and 患者免受此类事件的侵害。

在此，我们将了解加密的涵义、数据加密方法以及 Azure 上可用的加密功能。

# 什么是加密?

加密是使数据不可读且不可用的过程。必须进行解密（需要使用密钥），才能使用或读取加密数据。有两种顶级加密类型：对称和非对称。

对称加密使用相同的密钥来加密和解密数据。考虑使用密码管理器应用程序。输入用自己的个人密钥加密的密码。（密钥通常派生自主密码。）需要检索数据时，使用相同的密钥并解密数据。

非对称加密使用公钥和私钥对。任意一个密钥都可以加密但不能解密自己的加密数据。若要解密，则需要配对密钥。非对称加密用于诸如 TLS（用于 HTTPS）和数据签名等内容。

对称和非对称加密都在正确保护数据方面扮演重要角色。

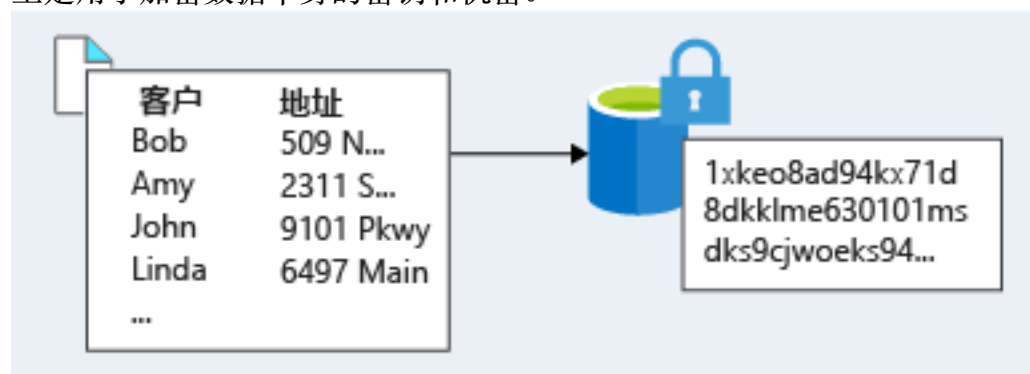
加密通常以两种方式进行：静态加密和传输中加密。

## 静态加密

静态数据是存储在物理介质上的数据。这可以是存储在服务器磁盘上的数据、存储在数据库中的数据或存储在存储帐户中的数据。

无论存储机制如何，静态数据加密都可确保在没有解密密钥和机密的情况下，存储的数据不可读。如果攻击者获取了包含加密数据的硬盘驱动器，但无法访问加密密钥，那么就很难盗用该数据。在这种情况下，攻击者只能尝试攻击加密数据，这比访问硬盘驱动器上的未加密数据要复杂得多，消耗的资源也多得多。

加密的数据可能会因其内容、使用情况和对组织的重要性而有所不同。它可能是对企业至关重要的财务信息、企业开发的知识产权、企业存储的关于客户或员工的个人数据，甚至是用于加密数据本身的密钥和机密。

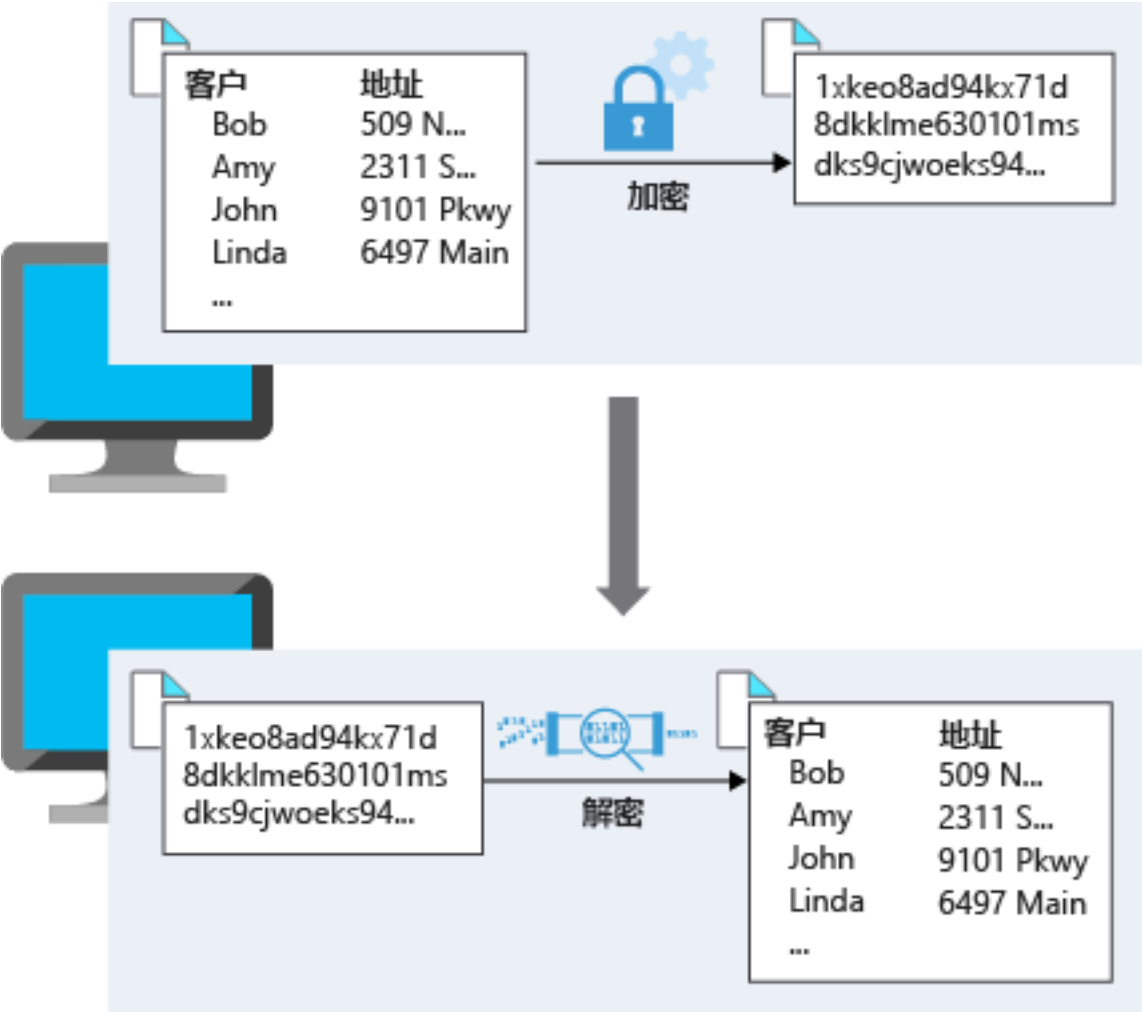


## 传输中加密

传输中的数据是主动从一个位置移动到另一个位置的数据，例如通过 Internet 或通过专用网络。组织可以通过以下方式处理安全传输：加密数据，然后通过网络进行发送，或者

设置安全通道以在两个系统之间传输未加密的数据。加密传输中数据可保护数据免受外部观察程序的影响，并提供传输数据的机制，同时降低暴露的风险。

下图是传输中加密的示例。在传输数据前，将对其进行加密。数据到达目标后，就会对其进行解密。



## 识别数据并对其进行分类

让我们重新审视你的组织试图解决的问题。该组织之前发生过泄露敏感数据的事件，因此加密的内容与应加密的内容之间存在差距。该组织需要首先识别他们存储的数据类型并对其进行分类，然后让其符合数据存储的业务和法规要求。

最好将此数据分类，因为它与组织、组织客户或组织合作伙伴的泄露影响有关。可按如下所示进行分类：

识别数据并对其进行分类

数据分类	说明	示例
受限制	分类为“受限制”的数据被泄露、篡改或删除后将产生重大风险。此数据需要强保护级别。	包含社会安全号码、信用卡号码、个人健康状况记录的数据
专用	分类为“专用”的数据被泄露、篡改或删除后将产生一定的风险。此数据需要合理的保护级别。未分类为“受限制”或“公开”的数据将分类为“专用”数据。	包含地址、电话号码、学术记录、客户购买记录等信息的个人记录
公开	分类为“公开”的数据被泄露、篡改或删除后将不构成风险。此数据不需要任何保护。	公共财务报告、公钥策略、客户产品文档

通过对存储的数据类型进行清点，组织可更好地了解可能存储敏感数据的位置以及可能使用或不使用现有加密的位置。

全面了解适用于组织存储的数据的法规和业务要求也很重要。组织必须遵守的法规要求通常会驱动大部分数据加密要求。

你的组织存储的是属于《健康保险可携性责任法案》(Health Insurance Portability and Accountability Act, HIPAA) 的敏感数据，该法案包含有关如何处理和存储患者数据的要求。其他行业有不同的法规要求。金融机构可能会存储属于支付卡行业 (PCI) 标准的帐户信息。在欧洲开展业务的组织可能属于一般数据保护条例 (GDPR) 的范畴，该法规定了在欧洲处理个人数据的方式。

业务要求还可能要求任何可能使组织面临财务风险的数据都需要加密。竞争信息就属于这一类别。

对数据进行分类并定义需求后，就可利用工具和技术在体系结构中实现和实施加密。

## Azure 上的加密

我们来看看使用 Azure 可在服务中加密数据的一些方法。

### 加密原始存储

静态数据的 Azure 存储加密有助于保护数据，使组织能够信守安全性与合规性方面所做的承诺。Azure 存储平台会在将数据保存到磁盘之前自动使用 256 位高级加密标准 (AES) 加密来加密数据，并在检索过程中解密这些数据。Azure 存储中的加密、静态加密、解密

和密钥管理的这种处理对于使用该服务的应用程序是透明的。无需添加任何代码或启用任何功能。

可以将 Microsoft 管理的加密密钥与 Azure 存储加密一起使用，也可以通过在 Azure 门户中选择对应的选项来使用自己的加密密钥。



Azure 存储会自动加密以下位置中的数据：

- 所有 Azure 存储服务，包括 Azure 托管磁盘、Azure Blob 存储、Azure 文件存储、Azure 队列存储和 Azure 表存储
- 两个性能层（标准层和高级层）
- 两个部署模型（Azure 资源管理器模型和经典模型）

对于你的组织，Azure 存储加密意味着每当有人使用支持 Azure 存储服务加密的服务时，其数据都会在存储物理介质上加密。如果有人访问物理磁盘，则数据将不可读。

## 加密虚拟机

Azure 存储可为写入物理磁盘的数据提供低级加密保护，但如何保护虚拟机 (VM) 的虚拟硬盘 (VHD)？如果恶意攻击者获得了 Azure 订阅的访问权限并泄露了虚拟机的 VHD，如何确保他们无法访问存储在 VHD 上的数据？

Azure 磁盘加密是用于帮助加密 Windows 和 Linux IaaS 虚拟机磁盘的功能。Azure 磁盘加密使用 Windows 的行业标准 BitLocker 功能和 Linux 的 DM-Crypt 功能，为 OS 和数据磁盘提供卷加密。此解决方案与 Azure Key Vault 集成，用于控制和管理磁盘加密密钥与机密。（并且可以使用 Azure 服务的托管标识访问密钥保管库。）

在标准和高级 VM 的所有 Azure 公共区域和 Azure 政府区域中，适用于 Windows IaaS 和 Linux VM 的磁盘加密已正式发布。磁盘加密管理解决方案可以解决以下业务需求：

- 使用行业标准的加密技术轻松保护 IaaS VM，满足组织的安全性与合规性要求。



- IaaS VM 会根据客户控制的密钥和策略启动。可在 Key Vault 中审核密钥和策略的使用方式。

此外，如果使用 Azure 安全中心，当 VM 未加密时，会收到警报。这些警报显示为“高严重性”，建议对这些 VM 进行加密。

虚拟机建议

总计

缺少磁盘加密

2 个 VM, 共 2 个

虚拟机

名称	加入	系统更新	反恶意软件	基线	磁盘加密
<div><div></div><div>ASC-VM1</div></div>	✓	✓	✓	✓	1
<div><div></div><div>ASC-VM2</div></div>	✓	✓	✓	✓	1

你的组织可将磁盘加密应用于其虚拟机，以确保存储在 VHD 上的任何数据都按照组织要求和合规性要求进行保护。由于启动盘也是加密的，组织可以控制和审核使用情况。

## 加密数据库

你的组织有多个数据库，用于存储需要更多保护的数据。组织已将许多数据库迁移到 Azure SQL 数据库，并希望确保相应数据在其中处于加密状态。组织希望确保，如果数据文件、日志文件或备份文件被盗，在没有对加密密钥的访问权限的情况下无法读取这些文件。

透明数据加密有助于保护 Azure SQL 数据库和 Azure 数据仓库免受恶意活动的威胁。它可执行静态数据库、关联备份和事务日志文件的实时加密和解密，无需更改应用程序。默认情况下，所有新部署的 Azure SQL 数据库均启用了透明数据加密。

透明数据加密使用称为数据库加密密钥的对称密钥来加密整个数据库的存储。默认情况下，Azure 为每个逻辑 SQL Server 实例提供唯一的加密密钥，并处理所有详细信息。

Azure Key Vault 中存储的密钥也支持创建自己的密钥。

由于透明数据加密默认启用，因此你的组织可以确信他们对存储在其数据库中的数据有适当的保护。

对于本地 SQL Server 数据库，你的组织已启用 SQL Server Always Encrypted 功能。

Always Encrypted 旨在保护敏感数据，如客户个人信息或财务数据。此功能可帮助客户端应用程序通过安装的驱动程序来处理 SQL Server 数据库外的加密和解密，从而保护静态和传输中的列数据。这让你的组织可以最大程度地减少数据泄露，因为数据库决不会处理未加密的数据。

Always Encrypted 客户端驱动程序执行加密和解密过程。它按需重写 T-SQL 查询，以加密传递给数据库的数据并解密结果，同时保持这些操作对应用程序透明。

# 加密机密

我们已了解到，加密服务均使用密钥来加密数据 and 对其进行解密。如何确密密钥本身是安全的？你还可能拥有密码、连接字符串或其他需要安全存储的敏感信息。

Azure Key Vault 是一项云服务，用作机密的安全存储。可以通过 Key Vault 创建多个安全的称为保管库的容器。这些保管库受硬件安全模块 (HSM) 的支持。保管库可以集中存储应用程序机密，降低安全信息意外丢失的可能性。Key Vault 还控制并记录外界对其所存储内容的访问。

Azure Key Vault 负责处理传输层安全性 (TLS) 证书的请求和续订事宜，以提供可靠的证书生命周期管理解决方案。Key Vault 旨在支持任何类型的机密。这些机密可以是密码、数据库凭证、API 密钥和证书。

由于可授予 Azure Active Directory 标识使用 Key Vault 机密的访问权限，因此使用 Azure 服务的托管标识的应用程序可以自动无缝地获取所需的机密。

你的组织可以使用 Key Vault 存储其所有敏感的应用程序信息。这些信息包括组织用来确保系统之间通信安全的 TLS 证书。

# 加密备份

如果也没有对系统每天的备份进行加密，那么对其所有数据进行加密对你的组织是没有帮助的。你的组织使用 Azure 备份来备份本地计算机和 Azure VM 中的数据。Azure 备份允许 IT 部门在粒度级别上备份和恢复数据。备份包括文件、文件夹、计算机系统状态和应用感知数据。

对辛勤的 IT 部门来说，好消息是这种情况下不需要执行任何工作，因为所有数据都以静态加密形式存储。Azure 备份使用 AES256 和由管理员配置的密码创建的密钥来加密本地备份。数据通过 HTTPS 安全地传输到 Azure。然后，将已加密的数据存储在磁盘上。

Azure VM 也会自动进行静态加密，因为它们对其磁盘使用 Azure 存储。

# 知识检测

1. 判断正误：只有 Windows 虚拟机才能使用 Azure 磁盘加密。

正确

错误

2. 以下哪一项是对数据进行分类时的考虑因素？

客户面临的风险级别（若数据暴露）

数据传输方法

数据是存储在虚拟机上还是存储在数据库中

存储的数据量

检查你的答案

**E**

**n**

**c**

**r**

**y**

**p**

**ti**

**o**

**n**

- 10 minutes

Data is an organization's most valuable and irreplaceable asset. Encryption serves as the last and strongest line of defense in a layered security strategy for data.

Imagine you work for a healthcare organization that stores large amounts of sensitive data. The organization recently experienced a breach that exposed the unencrypted sensitive data of patients. The organization is now fully aware that it has gaps in its data protection capabilities. It wants to understand how it could have better used encryption to protect itself and its patients from this type of incident.

Here, we'll take a look at what encryption is, how to approach the encryption of data, and what encryption capabilities are available on Azure.

## What is encryption?

Encryption is the process of making data unreadable and unusable. To use or read the encrypted data, it must be *decrypted*, which requires the use of a secret key. There are two top-level types of encryption: *symmetric* and *asymmetric*.

Symmetric encryption uses the same key to encrypt and decrypt the data. Consider a password manager application. You enter your passwords, and they're encrypted with your own personal key. (Your key is often derived from your master password.) When the data needs to be retrieved, the same key is used and the data is decrypted.

Asymmetric encryption uses a public key and private key pair. Either key can encrypt but can't decrypt its own encrypted data. To decrypt, you need the paired key. Asymmetric encryption is used for things like TLS (used in HTTPS) and data signing.

Both symmetric and asymmetric encryption play a role in properly securing your data.

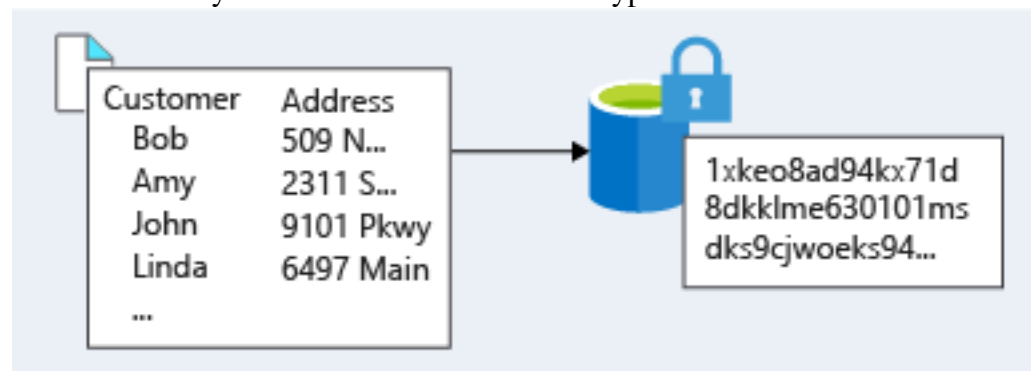
Encryption is typically approached in two ways: encryption at rest and encryption in transit.

## Encryption at rest

Data at rest is the data that has been stored on a physical medium. This might be data stored on the disk of a server, data stored in a database, or data stored in a storage account.

Regardless of the storage mechanism, encryption of data at rest ensures that the stored data is unreadable without the keys and secrets needed to decrypt it. If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, the attacker would have great difficulty compromising the data. In such a scenario, an attacker would have to attempt attacks against encrypted data, which is much more complex and resource consuming than accessing unencrypted data on a hard drive.

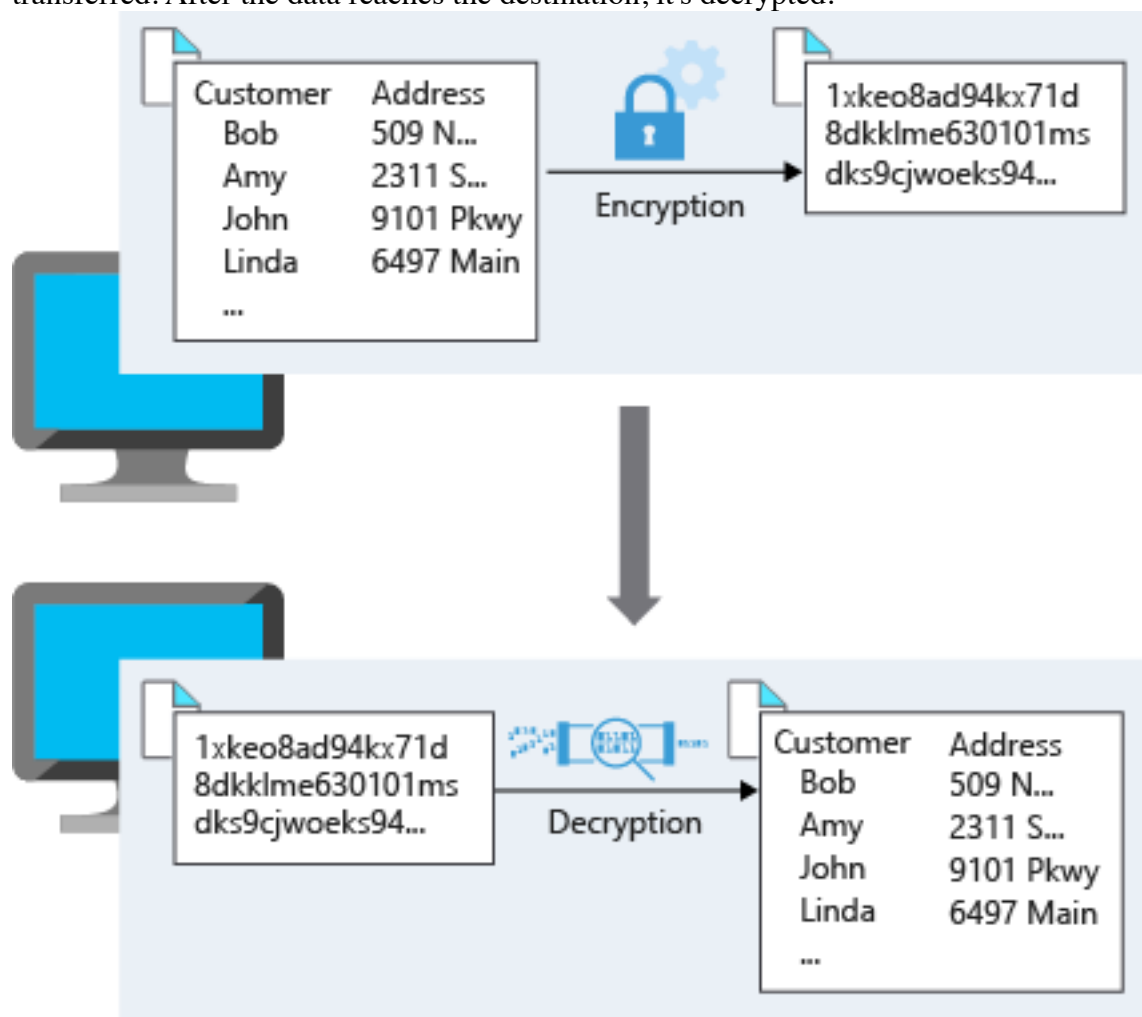
The data that's encrypted can vary in its content, usage, and importance to the organization. It might be financial information that's critical to the business, intellectual property that has been developed by the business, personal data that the business stores about customers or employees, and even the keys and secrets used for the encryption of the data itself.



## Encryption in transit

Data in transit is the data that's actively moving from one location to another, such as across the internet or through a private network. An organization can handle secure transfer by encrypting the data before sending it over a network, or setting up a secure channel to transmit unencrypted data between two systems. Encrypting data in transit protects the data from outside observers and provides a mechanism to transmit data while limiting risk of exposure.

The following illustration is an example of encryption in transit. The data is encrypted before it's transferred. After the data reaches the destination, it's decrypted.



## Identify and classify data

Let's revisit the problem that your organization is trying to solve. The organization has had previous incidents that exposed sensitive data, so there's a gap between what's being encrypted and what should be encrypted. The organization needs to start by identifying and classifying the types of data that it's storing, and align this with the business and regulatory requirements for the storage of data.

It's beneficial to classify this data as it relates to the impact of exposure to the organization, its customers, or its partners. An example classification might be as follows:

**IDENTIFY AND CLASSIFY DATA**

<b>Data classification</b>	<b>Explanation</b>	<b>Examples</b>
Restricted	Data classified as restricted poses significant risk if exposed, altered, or deleted. This data requires strong levels of protection.	Data that contains Social Security numbers, credit card numbers, personal health records
Private	Data classified as private poses moderate risk if exposed, altered, or deleted. This data requires reasonable levels of protection. Data that isn't classified as restricted or public will be classified as private.	Personal records that contain information such as address, phone number, academic records, customer purchase records
Public	Data classified as public poses no risk if exposed, altered, or deleted. This data doesn't require any protection.	Public financial reports, public policies, product documentation for customers

By taking an inventory of the types of data being stored, the organization can get a better picture of where sensitive data might be stored and where existing encryption might or might not be happening.

A thorough understanding of the regulatory and business requirements that apply to data that the organization stores is also important. The regulatory requirements that an organization must adhere to often drive a large part of the data encryption requirements.

Your organization is storing sensitive data that falls under the Health Insurance Portability and Accountability Act (HIPAA), which contains requirements on how to handle and store patient data. Other industries fall under different regulatory requirements. A financial institution might store account information that falls within Payment Card Industry (PCI) standards. An organization that does business in the EU might fall under the General Data Protection Regulation (GDPR), which defines the handling of personal data in the EU.

Business requirements might also dictate that any data that could put the organization at financial risk needs to be encrypted. Competitive information falls in this category.

After you've classified the data and defined your requirements, you can take advantage of tools and technologies to implement and enforce encryption in your architecture.

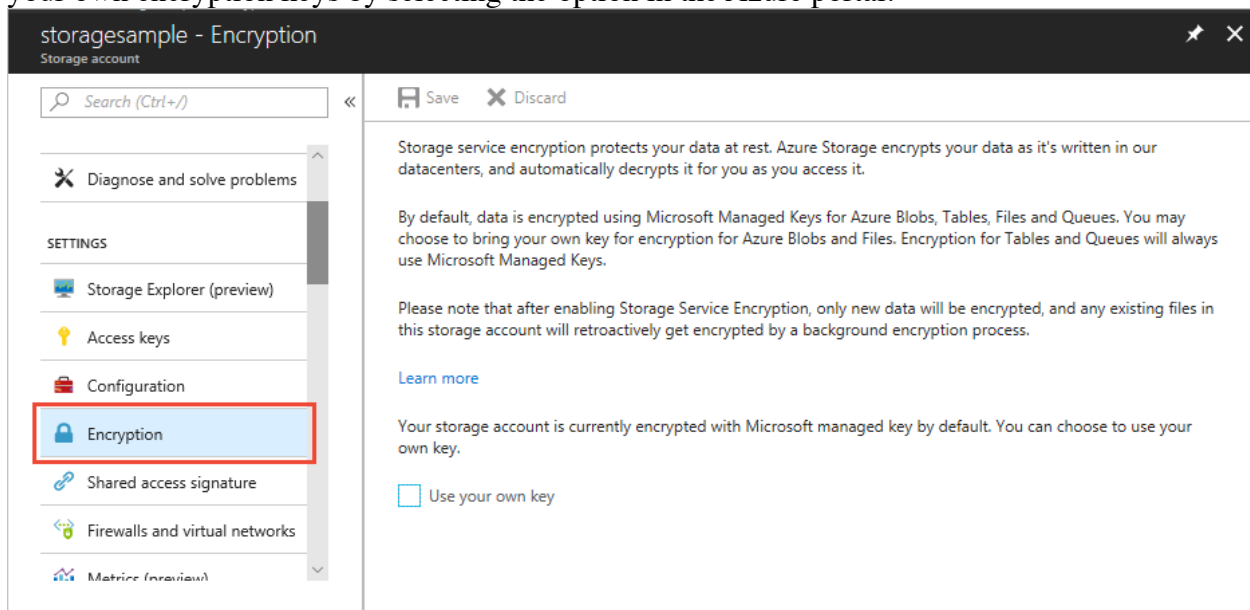
## Encryption on Azure

Let's take a look at some ways that Azure enables you to encrypt data across services.

### Encrypting raw storage

Azure Storage encryption for data at rest helps you protect your data to meet your organizational security and compliance commitments. The Azure Storage platform automatically encrypts your data with 256-bit Advanced Encryption Standard (AES) encryption before persisting it to disk and then decrypts the data during retrieval. This handling of encryption, encryption at rest, decryption, and key management in Azure Storage is transparent to applications that use the service. You don't need to add any code or turn on any features.

You can use Microsoft-managed encryption keys with Azure Storage encryption, or you can use your own encryption keys by selecting the option in the Azure portal.



Azure Storage automatically encrypts data in:

- All Azure Storage services, including Azure Managed Disks, Azure Blob Storage, Azure Files, Azure Queue Storage, and Azure Table Storage
- Both performance tiers (Standard and Premium)
- Both deployment models (Azure Resource Manager and classic)

For your organization, Azure Storage encryption means that whenever someone is using services that support Azure Storage encryption, their data is encrypted on the physical medium of storage. In the unlikely event that someone gets access to the physical disk, the data will be unreadable.

## Encrypting virtual machines

Azure Storage provides low-level encryption protection for data written to physical disk, but how do you protect the virtual hard disks (VHDs) of virtual machines (VMs)? If a malicious attacker gained access to your Azure subscription and exfiltrated the VHDs of your virtual machines, how would you ensure they'd be unable to access data stored on the VHD?

Azure Disk Encryption is a capability that 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 data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets. (And you can use managed identities for Azure services for accessing the key vault.)

Disk Encryption for Windows IaaS and Linux VMs is in general availability in all Azure public regions and Azure Government regions for Standard and Premium VMs. When you apply the Disk Encryption management solution, 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. You can audit their usage in your key vault.

In addition, if you use Azure Security Center, you're alerted if you have VMs that aren't encrypted. The alerts appear as High Severity, and the recommendation is to encrypt these VMs.

<

Your organization can apply Disk Encryption to its virtual machines to be sure that any data stored on VHDs is secured to organizational and compliance requirements. Because startup disks are also encrypted, the organization can control and audit usage.

## Encrypting databases

Your organization has several databases that store data that needs more protection. The organization has moved many databases to Azure SQL Database and wants to ensure that data is encrypted there. The organization wants to make sure that if the data files, log files, or backup files are stolen, they're unreadable without access to the encryption keys.

Transparent data encryption helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. By default, transparent data encryption is enabled for all newly deployed Azure SQL databases.

Transparent data encryption encrypts the storage of an entire database by using a symmetric key called the database encryption key. By default, Azure provides a unique encryption key per logical SQL Server instance and handles all the details. *Bring your own key* is also supported with keys stored in Azure Key Vault.

Because transparent data encryption is enabled by default, your organization can be confident that it has the proper protections in place for data stored in its databases.

For its on-premises SQL Server databases, your organization has turned on the SQL Server Always Encrypted feature. Always Encrypted is designed to protect sensitive data, such as client personal information or financial data. This feature helps protect column data at rest and in



transit by having the client application handle the encryption and decryption outside the SQL Server database through an installed driver. This allows your organization to minimize exposure of data, because the database never works with unencrypted data.

The Always Encrypted client driver performs the encryption and decryption processes. It rewrites the T-SQL queries as necessary to encrypt data passed to the database and decrypt the results, while keeping these operations transparent to the application.

## Encrypting secrets

We've seen that the encryption services all use keys to encrypt and decrypt data. How do we ensure that the keys themselves are secure? You might also have passwords, connection strings, or other sensitive pieces of information that you need to securely store.

Azure Key Vault is a cloud service that works as a secure store for secrets. Key Vault allows you to create multiple secure containers, called vaults. These vaults are backed by hardware security modules (HSMs). Vaults help reduce the chances of accidental loss of security information by centralizing the storage of application secrets. 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, to provide a robust certificate lifecycle management solution. Key Vault is designed to support any type of secret. These secrets can be passwords, database credentials, API keys, and certificates.

Because you can grant Azure Active Directory identities access to use Key Vault secrets, applications that use managed identities for Azure services can automatically and seamlessly acquire the secrets they need.

Your organization can use Key Vault for the storage of all of its sensitive application information. That information includes the TLS certificates that the organization uses to secure communication between systems.

## Encrypting backups

Encrypting all of its data won't help your organization if the daily backups of systems aren't also encrypted. Your organization uses Azure Backup to back up data from on-premises machines and Azure VMs. Azure Backup lets the IT department back up and recover data at a granular level. The backups include files, folders, machine system state, and app-aware data.

Luckily for your hard-working IT department, there's no work to do here because all the data is stored encrypted at rest. Azure Backup encrypts local backups by using AES256 and a key created from the passphrase configured by the administrator. The data is securely transferred to Azure through HTTPS. The already-encrypted data is then stored on disk. Azure VMs are also automatically encrypted at rest because they use Azure Storage for their disks.

## Check your knowledge

1. True or false: only Windows virtual machines can use Azure Disk Encryption.

True

False

2. When you're classifying data, which of the following is a factor?

Level of risk posed to customers if exposed

Method of data transport

Whether the data is stored on virtual machines or in a database

The amount of data stored

Check your answers

# 网络安全

- 10 分钟

保护网络免受攻击和未经授权的访问是任何体系结构的重要一环。在云迁移准备过程中，你的公司花时间规划了其网络基础结构。公司希望确保其拥有网络安全控制，以防止网络基础结构受到攻击。

在此，我们将了解什么是网络安全，如何将分层方法集成到体系结构中，以及 Azure 如何帮助你为环境提供网络安全。

## 什么是网络安全？

网络安全在于保护网络内外的资源通信。目标是限制服务和系统中网络层的泄露。通过限制此泄露，可降低资源受到攻击的可能性。为了实现网络安全，组织可以将其工作重点放在以下领域：

- 保护应用程序和 Internet 之间的流量流着重于限制网络外的泄露。网络攻击通常在网络外部开始，因此通过限制 Internet 泄露并保护外围，可以降低受到攻击的风险。

- 保护应用程序之间的流量流重点在于应用程序之间、其层级、不同环境之间以及网络中其他服务中的数据。通过限制这些资源之间的泄露，可以减少受损资源可能产生的影响。这有助于减少网络内的进一步传播。
- 保护用户与应用程序之间的流量流着重于保护用户的网络流。这限制了受外部攻击时资源的泄露，并为用户提供了一种安全机制来利用资源。

## 网络安全分层方法

整个模块中的常见线程是采用分层的安全方法，这种方法在网络层中也没有什么不同。仅仅专注于保护网络外围，或者专注于网络内部服务之间的网络安全是远远不够的。分层方法提供多级别保护，因此如果攻击者通过了一个层，就会有进一步的保护来限制进一步的攻击。

让我们来看看 Azure 如何为分层方法提供工具来保护你的网络足迹。

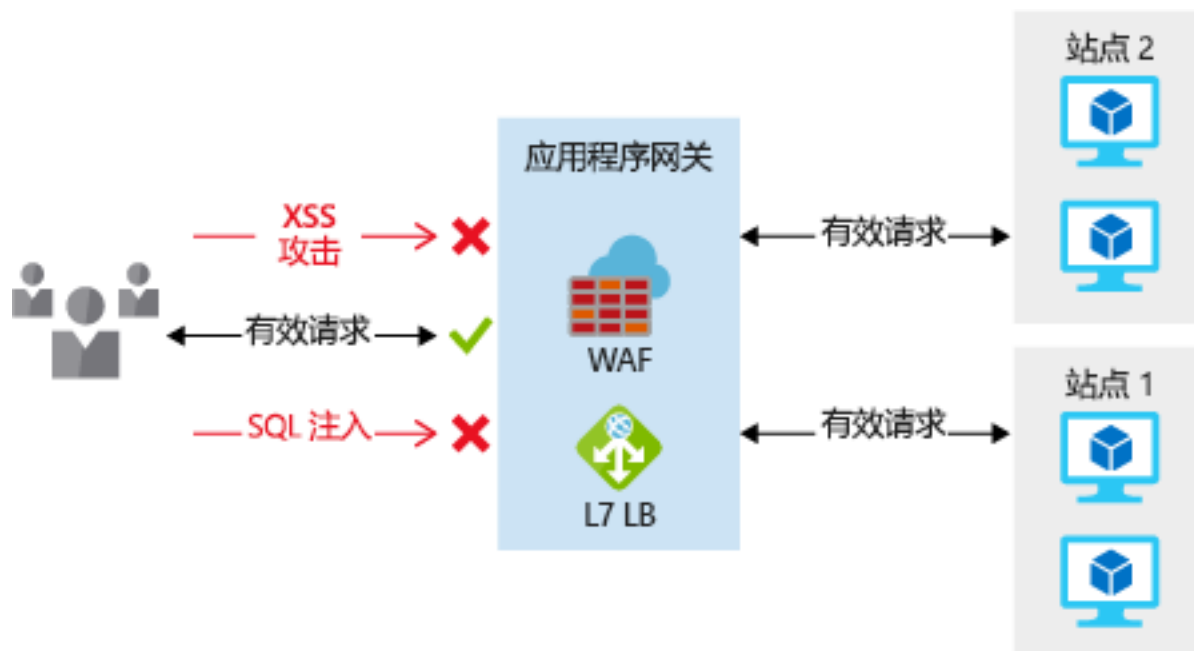
### Internet 保护

如果我们从网络的外围开始，关注的就是限制和消除来自 Internet 的攻击。一个好的起点是评估面向 Internet 的资源，并且只在必要时允许进站和出站通信。识别所有允许任何类型的进站网络流量的资源。确保这些资源是必需的，仅限于所需的端口和协议。

可在 Azure 安全中心查找此信息。安全中心将识别面向 Internet 的资源，这些资源没有与之相关的网络安全组。还将识别防火墙后不受保护的资源。

可通过几种方法在外围提供进站保护。Azure 应用程序网关是第 7 层负载均衡器，它也包括可为基于 HTTP 的服务提供高级安全性的 Web 应用程序防火墙 (WAF)。WAF 基于 OWASP 3.0 或 2.2.9 核心规则集中的规则。它提供针对常见已知漏洞（如跨站点脚本和 SQL 注入）的保护。

在下图中，应用程序网关的 WAF 功能保护系统免受恶意攻击。负载均衡器会在虚拟机之间分配合法请求。



为了保护基于非 HTTP 的服务或为了增加的自定义，可以使用网络虚拟设备 (NVA) 来保护网络资源。NVA 类似于可在本地网络中找到的防火墙设备，并且可从常用网络安全供应商处获得。NVA 可为需要它的应用程序提供更好的安全性自定义。但它们会增加复杂性，因此请仔细考虑你的要求。

任何向 Internet 公开的资源都有面临拒绝服务攻击攻击的风险。这些类型的攻击试图通过发送许多请求让资源变慢或无响应来导致网络资源瘫痪。

为了缓解这些攻击，Azure DDoS 防护为所有 Azure 服务提供了基本保护，并为资源的进一步自定义提供增强保护。DDoS 防护会阻止攻击流量并将合法流量转发至其预期目的地。在检测到攻击的几分钟内，系统会通过 Azure Monitor 指标通知你。

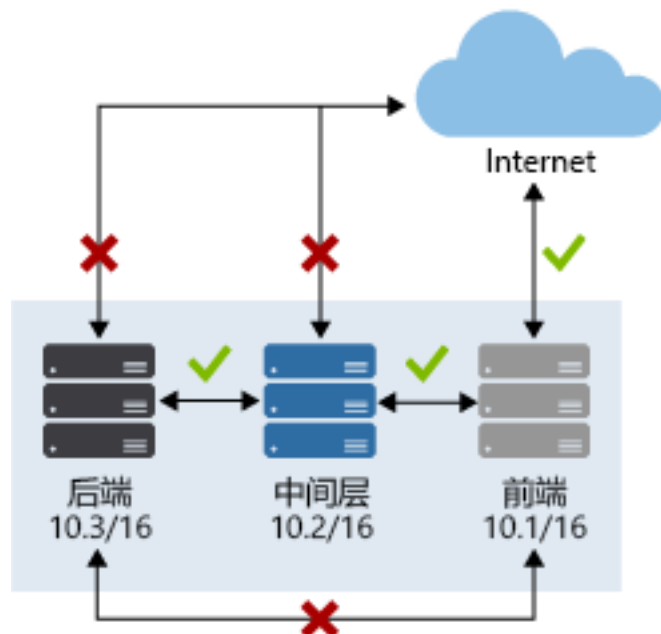


## 虚拟网络安全

进入虚拟网络后，请将资源之间的通信限制为仅需要的内容，这一点至关重要。

对于虚拟机之间的通信，网络安全组是限制不必要通信的关键一环。网络安全组在第 3 层和第 4 层上运行。它们提供了一个列表，其中包含进出网络接口和子网的允许通信和

拒绝通信。网络安全组是完全可自定义的，使你可以完全锁定与虚拟机往来的网络通信。通过使用网络安全组，可在环境、层级和服务之间隔离应用程序。下图显示了网络安全组如何限制后端和中间层直接与 Internet 通信。前端接收 Internet 请求，然后将其传递到中间层。中间层与后端进行通信。



若要将 Azure 服务隔离为仅允许来自虚拟网络的通信，请使用虚拟网络服务终结点。通过服务终结点，可在虚拟网络中保护 Azure 服务资源。

在虚拟网络中保护服务资源可以完全消除通过公共 Internet 对这些资源进行访问，只允许来自自己的虚拟网络的流量，从而提高了安全性。此方法具有以下好处：

- 减少环境的攻击面。
- 减少限制虚拟网络和 Azure 服务之间通信所需的管理。
- 为此通信提供最佳路由。

## 网络集成

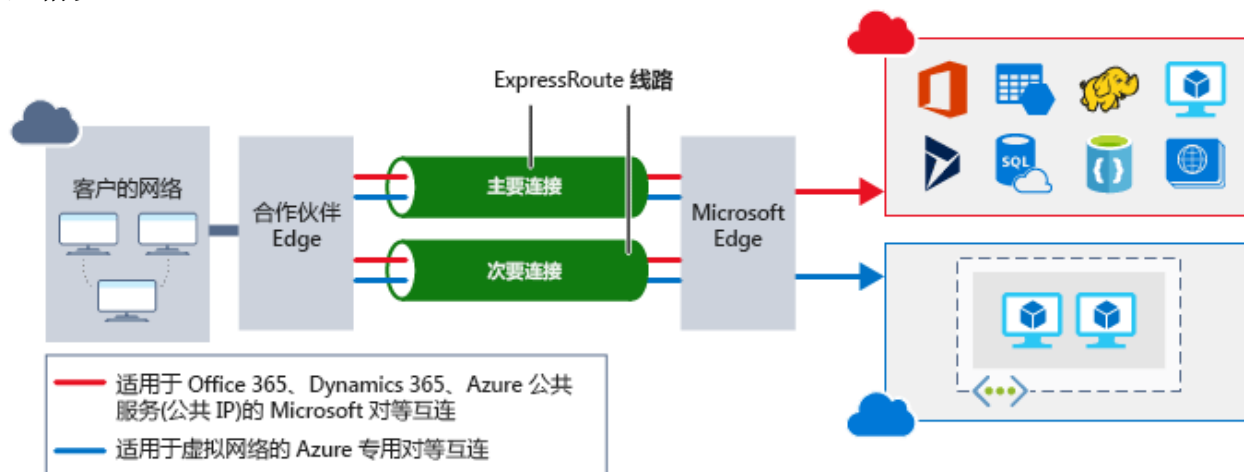
现有的网络基础结构通常需要集成以提供来自本地网络的通信，或者提供 Azure 中服务之间已改进的通信。有几种主要方法可处理这种集成并提高网络的安全性。

虚拟专用网 (VPN) 连接是在网络之间建立安全信道的常用方法。在 Azure 上使用虚拟网络时，这没有什么不同。Azure 虚拟网络与本地 VPN 设备之间的连接是在 Azure 上提供网络与虚拟机之间安全通信的好方法。

若要在网络和 Azure 之间提供专用连接，可使用 Azure ExpressRoute。使用 ExpressRoute 可通过连接由服务提供商辅助的专用连接，将本地网络扩展到 Microsoft 云。

使用 ExpressRoute 可与 Azure、Microsoft 365 和 Dynamics 365 等 Microsoft 云服务建立连接。这会使用专用线路而不是通过 Internet 发送此流量，从而提高本地通信的安全性。

无需允许用户通过 Internet 访问这些服务，而且可在设备之间发送此流量以进一步检查流量情况。



为了在 Azure 中轻松集成多个虚拟网络，虚拟网络对等互连在指定的虚拟网络之间建立直接连接。建立连接后，可使用网络安全组以与保护虚拟网络中资源相同的方式提供资源之间的隔离。通过此集成，可跨任何对等的虚拟网络提供相同的基本安全层。仅在直接连接的虚拟网络之间允许通信。

## 知识检查

1. Azure 网络安全组可用于保护以下哪些项之间的通信？

Azure 虚拟机与 Internet 之间的通信

虚拟网络中的 Azure 虚拟机之间的通信

本地网络中的 Azure 虚拟机和系统之间的通信

以上都是

2. 以下哪一项不是保护面向 Internet 的服务免受网络攻击的方法？

Azure DDoS 防护

Azure 应用程序网关 WAF

Azure 磁盘加密

网络虚拟设备

检查你的答案

# N e t w o r k s e c u r i t y

- 10 minutes

Securing your network from attacks and unauthorized access is an important part of any architecture. As part of preparation for its cloud migration, your company took the time to plan its network infrastructure. The company wanted to ensure that it had network security controls in place to protect the network infrastructure from attack.

Here, we'll look at what network security is, how to integrate a layered approach into your architecture, and how Azure can help you provide network security for your environment.

# What is network security?

Network security is protecting the communication of resources within and outside your network. The goal is to limit exposure at the network layer across your services and systems. By limiting this exposure, you decrease the likelihood that your resources can be attacked. For network security, an organization can focus its efforts on the following areas:

- *Securing traffic flow between applications and the internet* focuses on limiting exposure outside your network. Network attacks will most often start outside your network, so by limiting the internet exposure and securing the perimeter, you can reduce the risk of being attacked.
- *Securing traffic flow among applications* focuses on data between applications and their tiers, between different environments, and in other services within your network. By limiting exposure between these resources, you reduce the effect that a compromised resource can have. This can help reduce further propagation within the network.
- *Securing traffic flow between users and an application* focuses on securing the network flow for your users. This limits the exposure that your resources have to outside attacks, and it provides a secure mechanism for users to utilize your resources.

## Layered approach to network security

A common thread throughout this module has been taking a layered approach to security, and this approach is no different at the network layer. It's not enough to just focus on securing the network perimeter, or focusing on the network security between services inside a network. A layered approach provides multiple levels of protection so that if an attacker gets through one layer, further protections are in place to limit the attack.

Let's look at how Azure can provide the tools for a layered approach to securing your network footprint.

## Internet protection

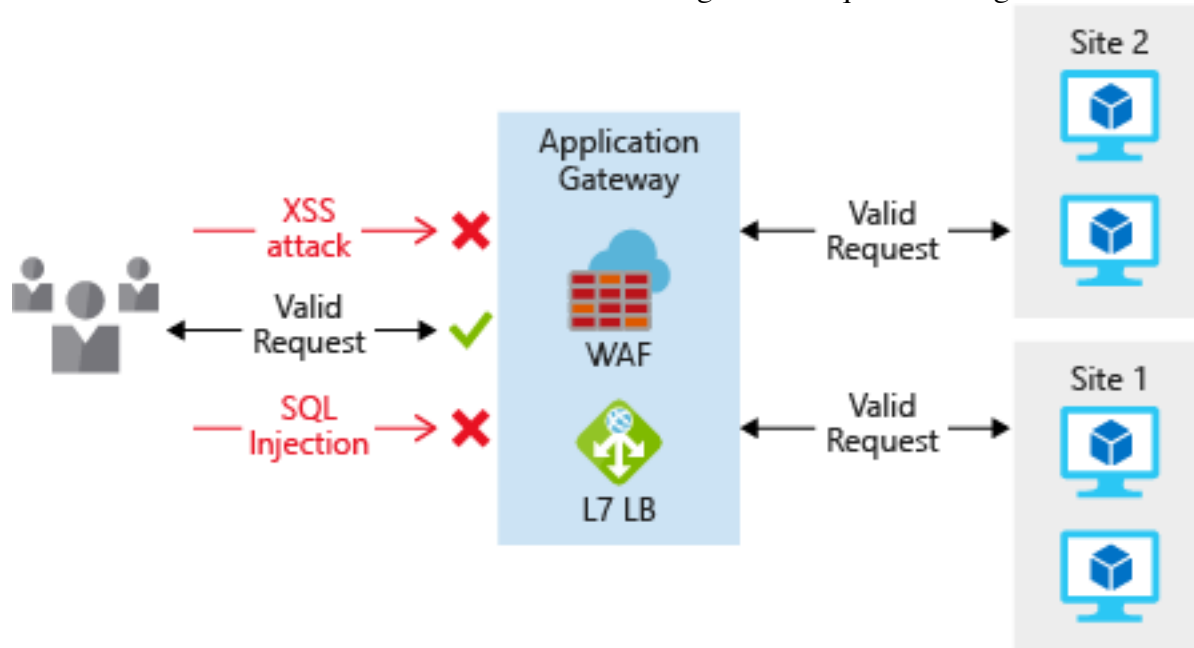
If you start on the perimeter of the network, you're focused on limiting and eliminating attacks from the internet. A great place to start is to assess the resources that are internet-facing, and allow inbound and outbound communication only where necessary. Identify all resources that are allowing inbound network traffic of any type. Ensure that they're necessary and restricted to only the required ports and protocols.

You can look for this information in Azure Security Center. Security Center will identify internet-facing resources that don't have network security groups associated with them. It will also identify resources that aren't secured behind a firewall.

There are a couple of ways to provide inbound protection at the perimeter. Azure Application Gateway is a Layer 7 load balancer that also includes a web application firewall (WAF) to provide advanced security for your HTTP-based services. The WAF is based on rules from the OWASP 3.0 or 2.2.9 core rule sets. It provides protection from commonly known vulnerabilities such as cross-site scripting and SQL injection.



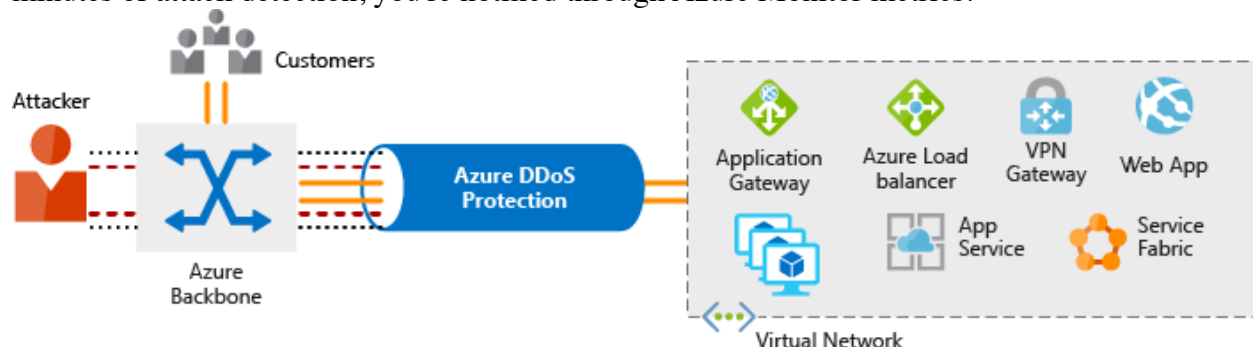
In the following diagram, the WAF feature of the application gateway protects the system from malicious attacks. The load balancer distributes the legitimate requests among virtual machines.



For protection of non-HTTP-based services or for increased customization, you can use network virtual appliances (NVAs) to secure your network resources. NVAs are similar to firewall appliances that you might find in on-premises networks, and are available from popular network security vendors. NVAs can provide greater customization of security for those applications that require it. But they increase complexity, so we recommend that you carefully consider your requirements.

Any resource exposed to the internet is at risk for a denial-of-service attack. These types of attacks try to overwhelm a network resource by sending so many requests that the resource becomes slow or unresponsive.

To mitigate these attacks, Azure DDoS Protection provides basic protection across all Azure services and enhanced protection for further customization for your resources. DDoS Protection blocks attack traffic and forwards legitimate traffic to its intended destination. Within a few minutes of attack detection, you're notified through Azure Monitor metrics.

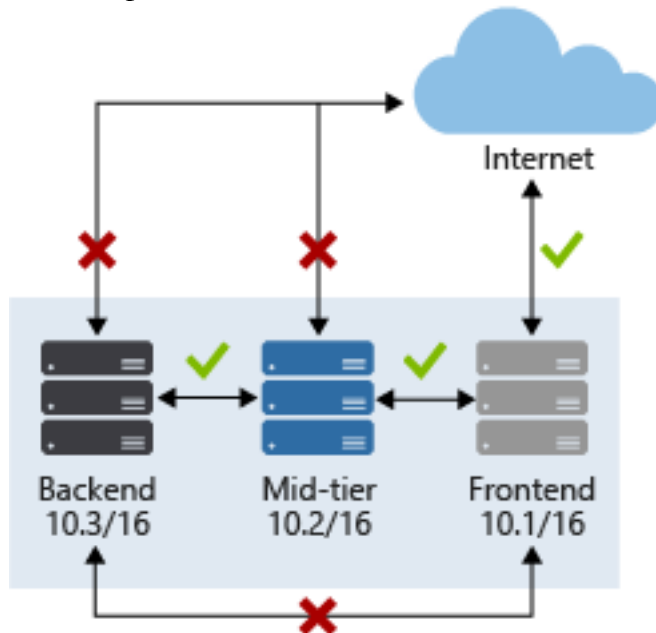


## Virtual network security

Inside a virtual network, it's important to limit communication between resources to only what's required.

For communication between virtual machines, network security groups are a critical piece to restrict unnecessary communication. Network security groups operate at layers 3 and 4. They provide a list of allowed and denied communication to and from network interfaces and subnets. Network security groups are fully customizable, and they enable you to lock down network communication to and from your virtual machines. By using network security groups, you can isolate applications between environments, tiers, and services.

The following diagram shows how a network security group restricts the back end and middle tier from communicating directly with the internet. The front end receives the internet requests and then passes them to the middle tier. The middle tier communicates with the back end.



To isolate Azure services to allow communication only from virtual networks, use virtual network service endpoints. With service endpoints, you can secure Azure service resources 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. This technique:

- Reduces the attack surface for your environment.
- Reduces the administration required to limit communication between your virtual network and Azure services.
- Provides optimal routing for this communication.

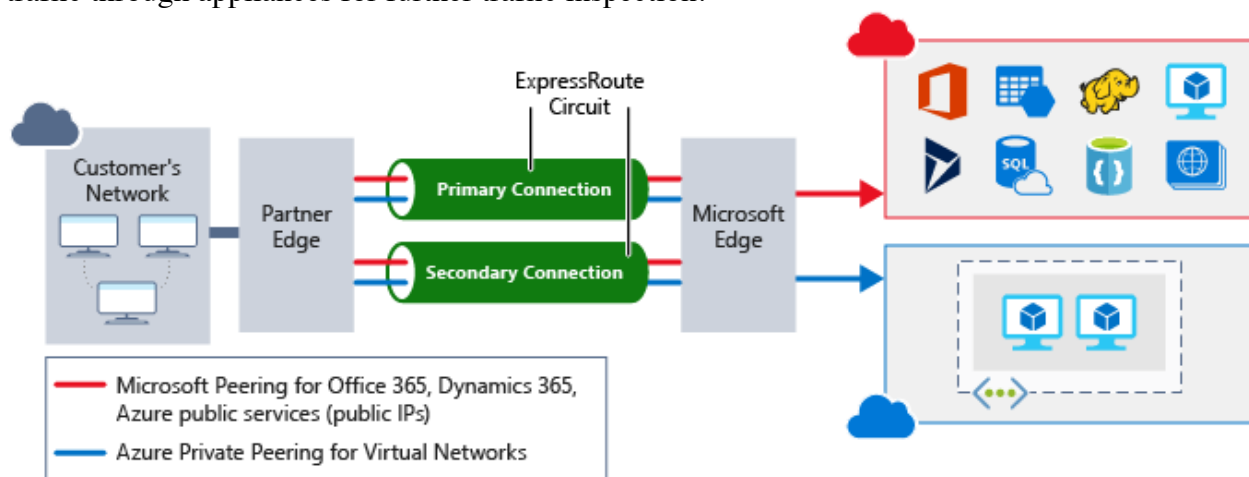
## Network integration

It's common to have existing network infrastructure that needs to be integrated to provide communication from on-premises networks, or to provide improved communication between services in Azure. There are a few key ways to handle this integration and improve the security of your network.

Virtual private network (VPN) connections are a common way of establishing secure communication channels between networks. This is no different when you're working with virtual networking on Azure. Connection between Azure virtual networks and an on-premises VPN device is a great way to provide secure communication between your network and your virtual machines on Azure.

To provide a dedicated, private connection between your network and Azure, you can use Azure ExpressRoute. 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, such as Azure, Microsoft 365, and Dynamics 365. This improves the security of your on-premises communication by sending this traffic over the private circuit instead of over the internet. You don't need to allow access to these services for your users over the internet, and you can send this traffic through appliances for further traffic inspection.



To easily integrate multiple virtual networks in Azure, virtual network peering establishes a direct connection between designated virtual networks. After a connection is established, you can use network security groups to provide isolation between resources in the same way that you secure resources within a virtual network. This integration gives you the ability to provide the same fundamental layer of security across any peered virtual networks. Communication is allowed only between directly connected virtual networks.

## Check your knowledge

1. Azure network security groups can be used to secure communication between which of the following?

Communication between Azure virtual machines and the internet

Communication between Azure virtual machines within a virtual network

Communication between Azure virtual machines and systems in an on-premises network

All of the above

2. Which of the following is not a method for protecting internet-facing services from network attacks?

Azure DDoS Protection

Azure Application Gateway WAF

Azure Disk Encryption

A network virtual appliance

Check your answers

# 应用程序安全性

• 8 分钟

在云平台上托管应用程序比传统的本地部署更具有优势。云的责任共担模型在云提供商的控制下移动物理网络、生成和主机级别的安全性。对比相当多的投资和见解提供商都纷纷加入保护并监视其基础结构的行列，试图在此级别入侵平台的攻击者会看到收益递减。

攻击者能更有效地追踪云平台客户在应用程序级别引入的漏洞。此外，通过采用平台即服务 (PaaS) 来托管其应用程序，客户可从管理操作系统安全性中释放资源，将其部署为强化应用程序代码并监视应用程序周围的标识外围。在此处，我们将讨论可通过设计改进应用程序安全性的一些方法。

## 场景

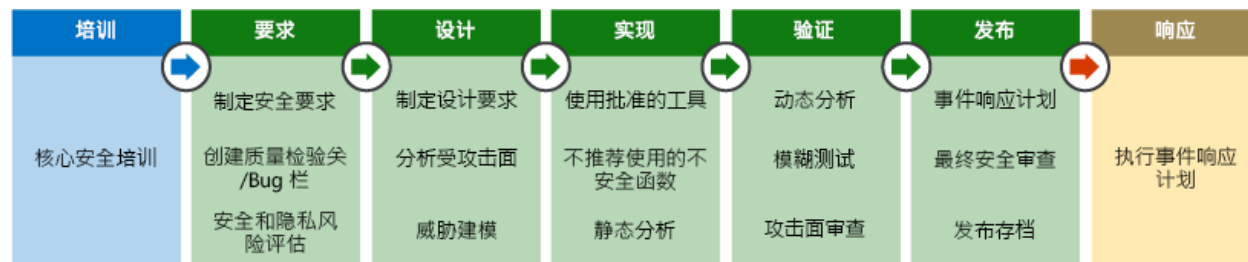
假设你在一个医疗保健组织中工作，其客户需要通过联机 Web 门户访问其个人医疗记录。强制遵守《健康保险可携性责任法案》(Health Insurance Portability and Accountability Act, HIPAA)，如果发生个人数据安全漏洞，公司将面临重大的经济处罚风险。保护与其交互的应用程序和个人数据至关重要。

与客户应用程序相关的主要方面包括：

- 安全的应用程序设计
- 数据安全性
- 标识和访问管理
- 终结点安全性

## 安全开发生命周期

可在应用程序设计阶段使用 Microsoft 安全开发生命周期 (SDL) 进程，以确保在软件开发生命周期中包含安全问题。设计应用程序时，更容易解决安全性和合规性问题，并且能缓解可能导致最终产品存在安全漏洞的许多常见错误。在软件开发过程早期解决问题的成本也要低得多。软件项目可使用此典型 SDL 步骤顺序：



从文化观点来看，SDL 相当于一个过程或一套工具。构建一种文化，其中安全性是主要关注点，并且任何应用程序开发的要求都可围绕安全性在发展组织能力方面取得重大进展。

## 运营安全评估

部署应用程序后，必须不断评估其安全状况，确定如何缓解发现的任何问题并将知识反馈回软件开发周期中。组织执行此评估的深度是软件开发和运营团队成熟度以及数据隐私要求的一个因素。扫描安全漏洞的软件服务可以帮助自动执行此过程并定期评估安全问题。此类服务提供了这些好处，使团队不用花费高昂的成本执行手动过程，如渗透测试。

Azure 安全中心是一项免费服务，现在默认针对所有 Azure 订阅启用。它可与其他 Azure 应用程序级别服务（如 Azure 应用程序网关和 Azure Web 应用程序防火墙）紧密集成。通过分析这些服务中的日志，安全中心可实时报告已知漏洞，提出关于缓解这些漏洞的应对建议。甚至可将安全中心配置为自动执行 playbook 以应对攻击。

## 标识用作外围

标识验证正成为应用程序的第一道防线。通过身份验证和授权会话来限制对 Web 应用的访问可大大减少攻击外围应用的情况。

Azure Active Directory (Azure AD) 和 Azure Active Directory B2C (Azure AD B2C) 提供了一种有效的方法来摆脱标识和访问完全托管服务的责任。Azure AD 条件访问策略、Privileged Identity Management 和标识保护控制进一步增强了防止未授权访问和审核更改的能力。

## 数据保护

如果存在不是针对 Web 应用的攻击，那么这些大部分攻击都是针对客户数据。因此，在应用程序及其数据存储层之间安全存储和传输数据至关重要。

你的组织存储和访问敏感患者医疗记录数据。1996 年由美国国会颁布的 HIPAA 以及其他控制措施定义了医疗保健提供商和雇主进行电子医疗保健交易的国家/地区标准。医疗保健提供商必须确保患者和被授权方（例如他们的医生）能够安全地访问医疗数据。为了满足这些要求，你的组织已经修改了其应用程序，以加密静态和传输中的所有患者数据。例如，组织使用传输层安全性 (TLS) 加密 Web 应用程序和后端 SQL 数据库之间交换的数据。还可以通过透明数据加密在 SQL Server 中静态加密数据。静态加密可确保即使环境受到入侵，如果没有正确的解密密钥，数据对任何人实际上也是无用的。

若要加密存储在 Azure Blob 存储中的数据，可以使用客户端加密对内存中的数据进行加密，然后再将其写入存储服务。支持此加密的库可用于 .NET、Java 和 Python。这些库可将数据加密直接集成到应用程序中，以增强数据完整性。

## 安全密钥和机密存储

从用于访问数据的应用程序中分离应用程序机密（如连接字符串或密码）和加密密钥，这至关重要。加密密钥和应用程序机密不应存储在应用程序代码或配置文件中。

请改用 Azure Key Vault 等安全存储。然后，可以通过 Azure 资源托管标识将此敏感数据的访问权限限制为应用程序标识。如果加密密钥泄露，则可以定期轮换密钥以防止泄露。

还可以选择使用本地硬件安全模块 (HSM) 生成的你自己的加密密钥。甚至可以要求在单个租户的离散 HSM 中实现 Azure Key Vault 实例。

下一单元: 总结

# A p p l i c a t i o n s e c u r i t y

• 8 minutes



Hosting applications on a cloud platform provides advantages over traditional on-premises deployments. The cloud's shared-responsibility model moves security at the physical network, building, and host levels under the control of the cloud provider. An attacker who tries to compromise the platform at this level would see diminishing returns versus the considerable investment and insight that providers make in securing and monitoring their infrastructure.

It's far more effective for attackers to pursue vulnerabilities introduced at the application level by cloud-platform customers. Furthermore, by adopting platform as a service (PaaS) to host their applications, customers can free resources from managing operating system security and deploy them to harden application code and monitor the identity perimeter around the application. Here, we'll discuss some of the ways that you can improve application security through design.

## **Scenario**

Imagine you work for a healthcare organization whose customers require access to their personal medical records through an online web portal. Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is mandatory and puts the company at significant risk of financial penalties if a breach of personal data occurs. Securing the application and personal data that it interacts with is paramount.

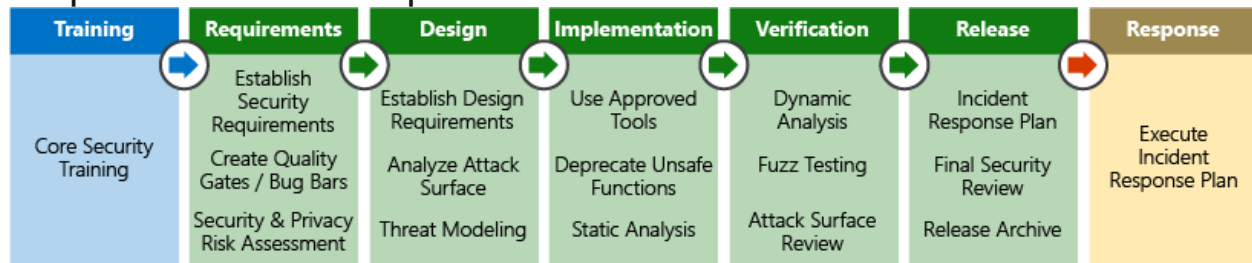
The primary areas that concern customer applications are:

- Secure application design
- Data security
- Identity and access management
- Endpoint security

## **Security Development Lifecycle**

You can use the Microsoft Security Development Lifecycle (SDL) process during the application design stage to ensure that security concerns are incorporated in the software development

lifecycle. Security and compliance issues are far easier to address when you're designing an application and can mitigate many common errors that can lead to security flaws in the final product. Fixing issues early in the software development journey is also far less costly. A software project can use this typical sequence of SDL steps:



The SDL is as much a cultural aspect as it is a process or set of tools. Building a culture where security is a primary focus and requirement of any application development can make great strides in evolving an organization's capabilities around security.

## Operational security assessment

After an application has been deployed, it's essential to continually evaluate its security posture, determine how to mitigate any issues that are discovered, and feed the knowledge back into the software development cycle. The depth to which an organization performs this evaluation is a factor of the maturity level of the software development and operational teams as well as the data privacy requirements.

Software services that scan for security vulnerabilities are available to help automate this process and assess security concerns on a regular cadence. Such services offer these benefits without burdening teams with costly manual processes, such as penetration testing.

Azure Security Center is a free service that's now enabled by default for all Azure subscriptions. It's tightly integrated with other Azure application-level services, such as Azure Application Gateway and Azure Web Application Firewall. By analyzing logs from these services, Security Center can report on known

vulnerabilities in real time and recommend responses to mitigate them. You can even configure Security Center to automatically execute playbooks in response to attacks.

## **Identity as the perimeter**

Identity validation is becoming the first line of defense for applications. Restricting access to a web application by authenticating and authorizing sessions can drastically reduce the attack surface area.

Azure Active Directory (Azure AD) and Azure Active Directory B2C (Azure AD B2C) offer an effective way to offload the responsibility of identity and access to a fully managed service. Azure AD conditional access policies, Privileged Identity Management, and identity protection controls further enhance your ability to prevent unauthorized access and audit changes.

## **Data protection**

Customer data is the target for most, if not all, attacks against web applications. The secure storage and transport of data between an application and its data storage layer is paramount. Your organization stores and accesses sensitive patient medical record data. HIPAA, enacted by the United States Congress in 1996, among other controls, defines the national standards for electronic healthcare transactions by healthcare providers and employers. Healthcare providers and employers must ensure that patients and authorized parties, such as physicians, have secure access to medical data.

To comply with these requirements, your organization has modified its applications to encrypt all patient data at rest and in transit. For example, the organization uses Transport Layer Security (TLS) to encrypt data exchanged between the web application and back-end SQL databases. Data is also encrypted at rest in SQL Server through transparent data encryption. Encryption at rest ensures that even if the environment is

compromised, data is effectively useless to anyone without the correct decryption keys.

To encrypt data stored in Azure Blob Storage, you can use client-side encryption to encrypt the data in memory before it's written to the storage service. Libraries that support this encryption are available for .NET, Java, and Python. These libraries enable the integration of data encryption directly into applications to enhance data integrity.

## **Secure key and secret storage**

Separating application secrets (like connection strings or passwords) and encryption keys from the application that's used to access data is vital. Encryption keys and application secrets should never be stored in the application code or configuration files.

Instead, use a secure store such as Azure Key Vault. Access to this sensitive data can then be limited to application identities through managed identities for Azure resources. You can rotate keys on a regular basis to limit exposure if encryption keys are leaked.

You can also choose to use your own encryption keys generated by on-premises hardware security modules (HSMs). You can even mandate that Azure Key Vault instances are implemented in single-tenant, discrete HSMs.