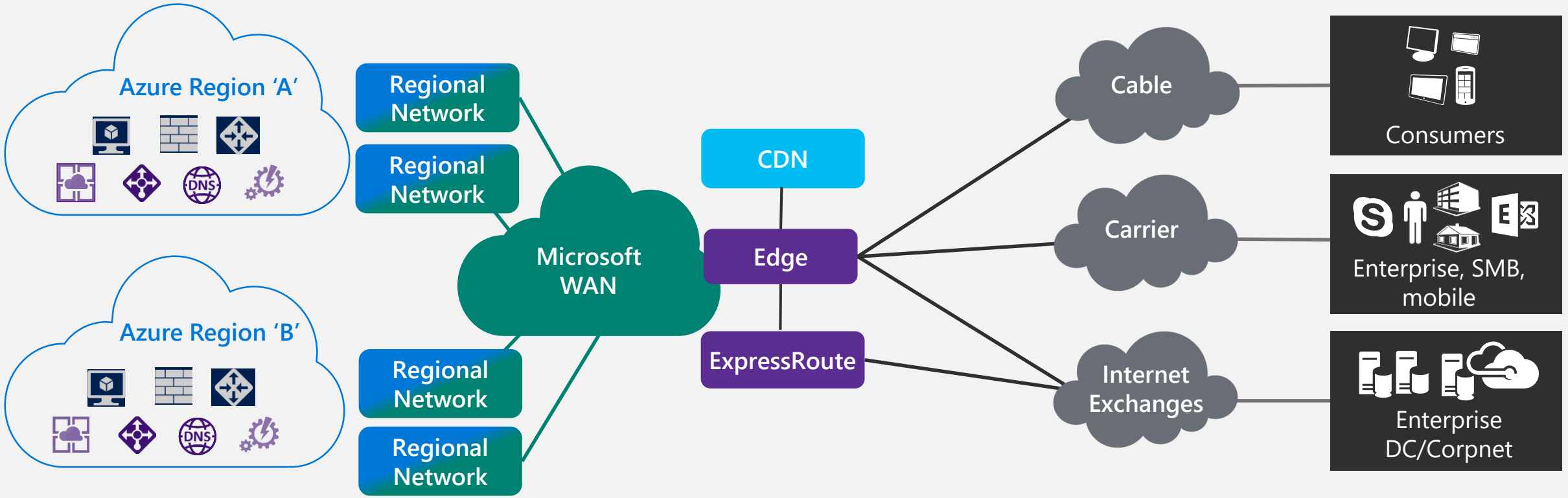
Azure安全根基 —— 虚拟机/网络/存储

Yi Liang
China OCP PTS
yiliang@microsoft.com

Azure Networking



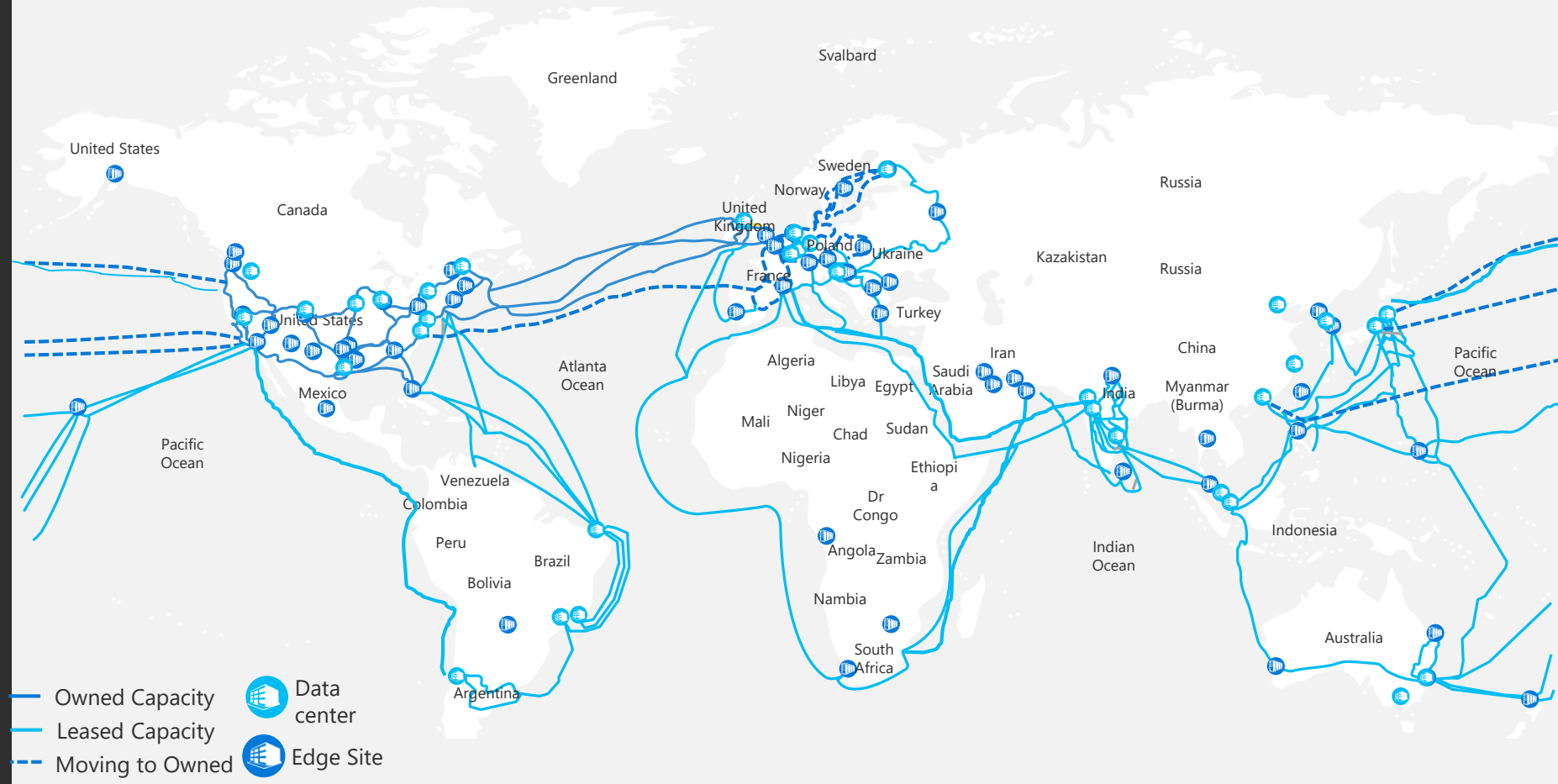
DC Hardware	Services	Intra-Region	WAN Backbone	Edge and ExpressRoute	CDN	Last Mile
• SmartNIC/FPGA • SONiC	• Virtual Networks • Load Balancing • VPN Services • Firewall • DDoS Protection • DNS & Traffic Management	• DC Networks • Regional Networks • Optical Modules	• Software WAN • Subsea Cables • Terrestrial Fiber • National Clouds	• Internet Peering • ExpressRoute	• Acceleration for applications and content	• E2E monitoring (Network Watcher, Network Performance Monitoring)

微软全球网络

拥有全球最大的光纤主干网络

- 8,000+ ISP sessions
- 130+ edge sites
- 44 ExpressRoute locations
- 33,000 miles of lit fiber
- SDN Managed (SWAN, OLS)

DCs and Network sites not exhaustive

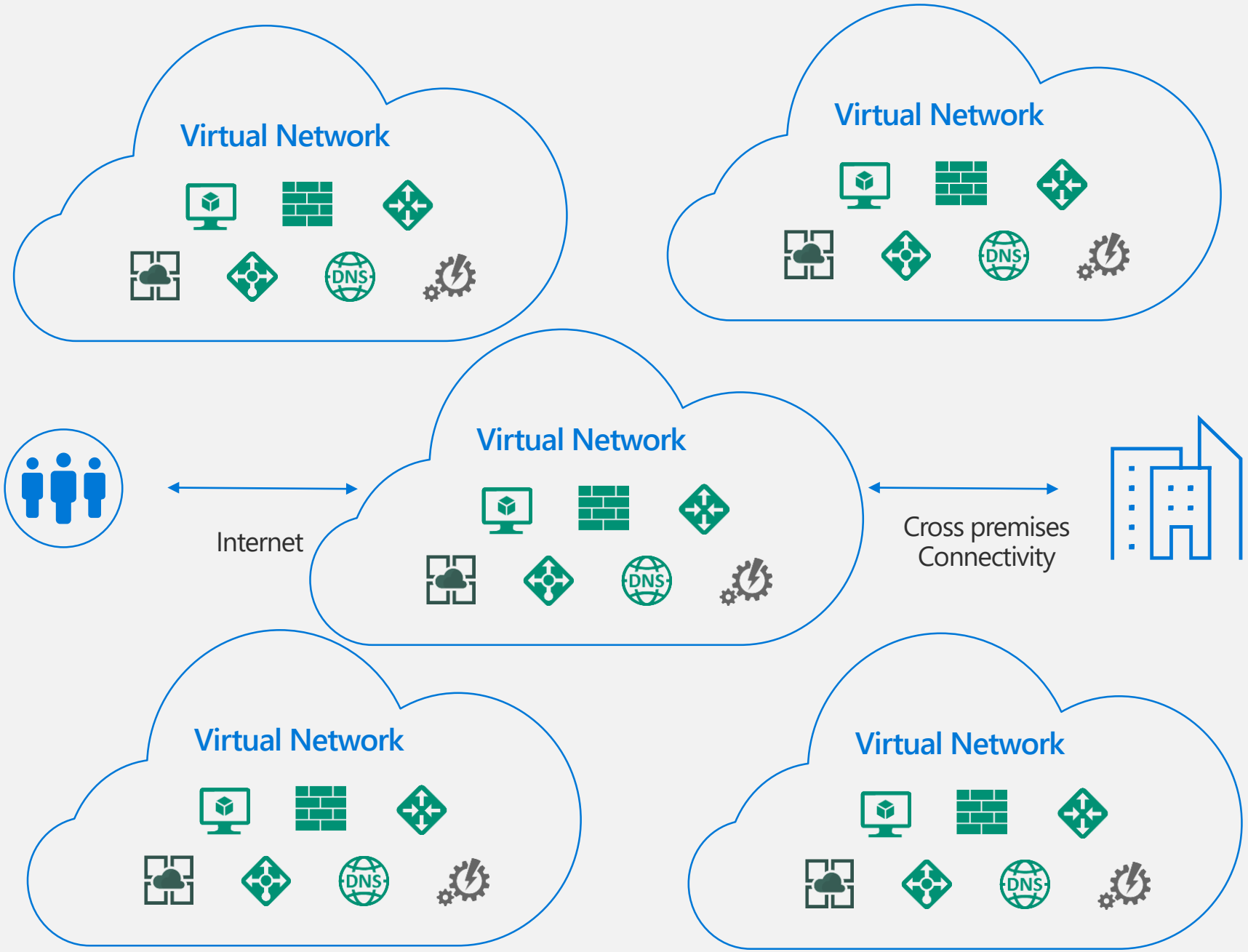


即刻构建属于您的Azure虚拟网络

为每位客户在云中构建属于自己的虚拟数据中心

可以在几分钟内实例化和配置复杂拓扑

丰富的安全和网络服务

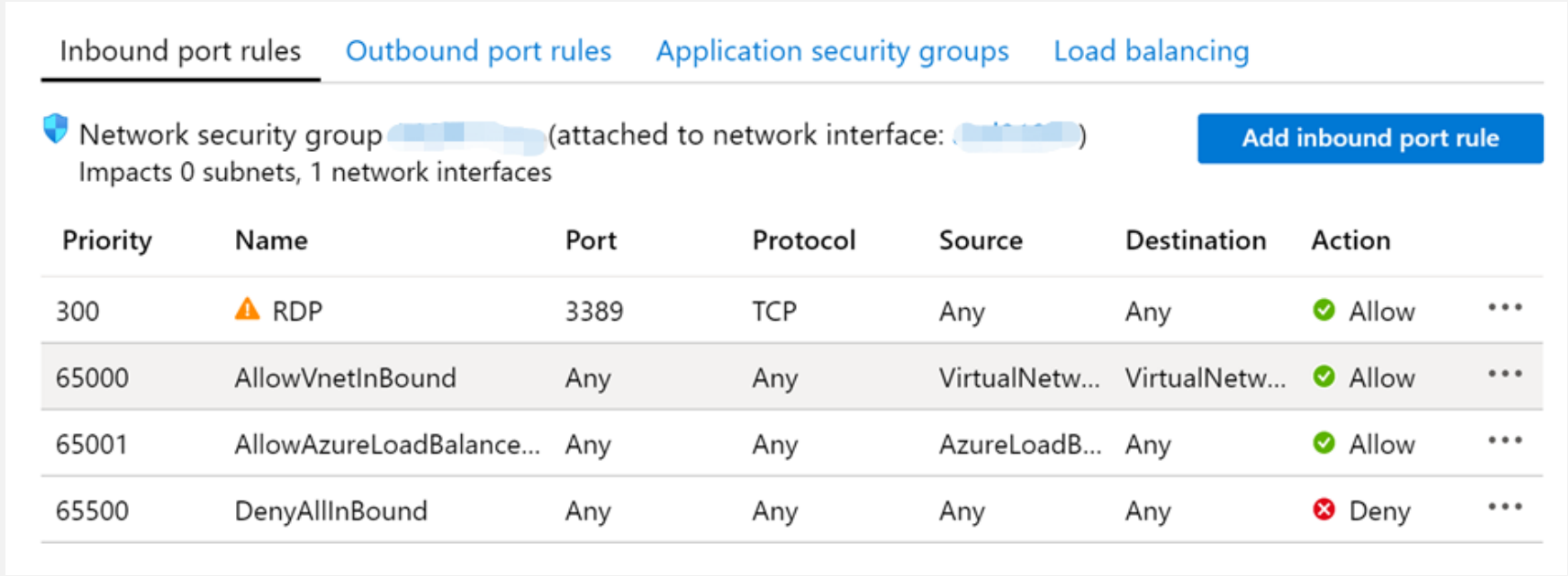


网络安全加固

- 网络安全组
- Azure防火墙
- Web应用程序防火墙
- 远程访问和跨界连接
- 外围网络架构
- Azure DDoS防护
- 总结与补充

网络安全组(NSG)

- 静态数据包筛选防火墙，提供基本的网络级别访问控制（基于IP地址和TCP或UDP协议）
- 用户可以通过配置网络安全组规则自定义网络流量的筛选条件
- NSG可以与虚拟网络子网关联，同时也可以与子网中具体的网卡相关联，二者可以同时存在（在同时配置时，要避免二者冲突）



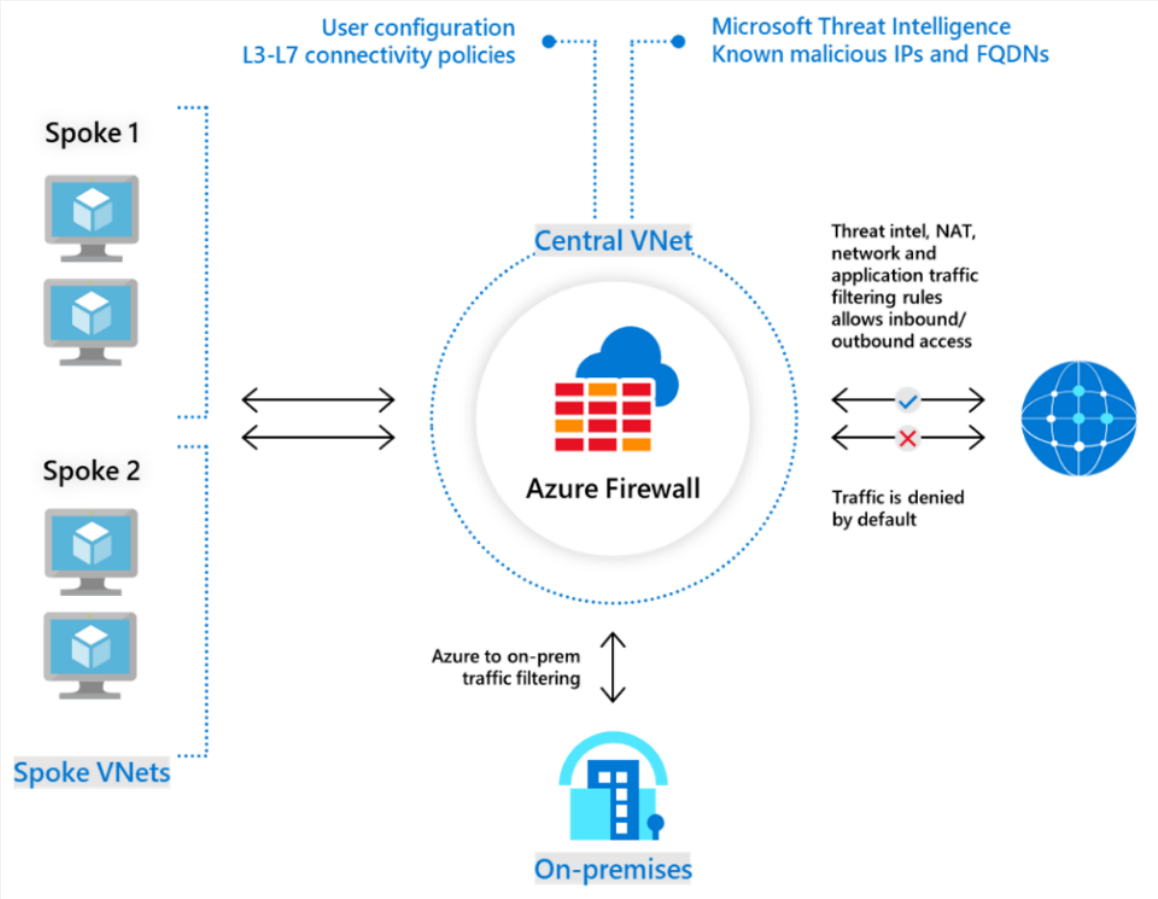
网络安全加固

- 网络安全组
- Azure 防火墙
- Web应用程序防火墙
- 远程访问和跨界连接
- 外围网络架构
- Azure DDoS防护
- 总结与补充

Azure 防火墙

网络安全组提供分布式网络层流量过滤，以限制每个订阅中虚拟网络内资源的访问流量。如果用户需要**跨订阅**，**跨虚拟网络**，启用某些**应用程序级别**的保护时，则需要使用Azure防火墙服务。

- 内置的高可用性
- 不受限制的云可伸缩性
- 应用程序FQDN筛选规则
- 支持源和目的网络地址转换
- 与 Azure Monitor完全集成
- 支持混合部署

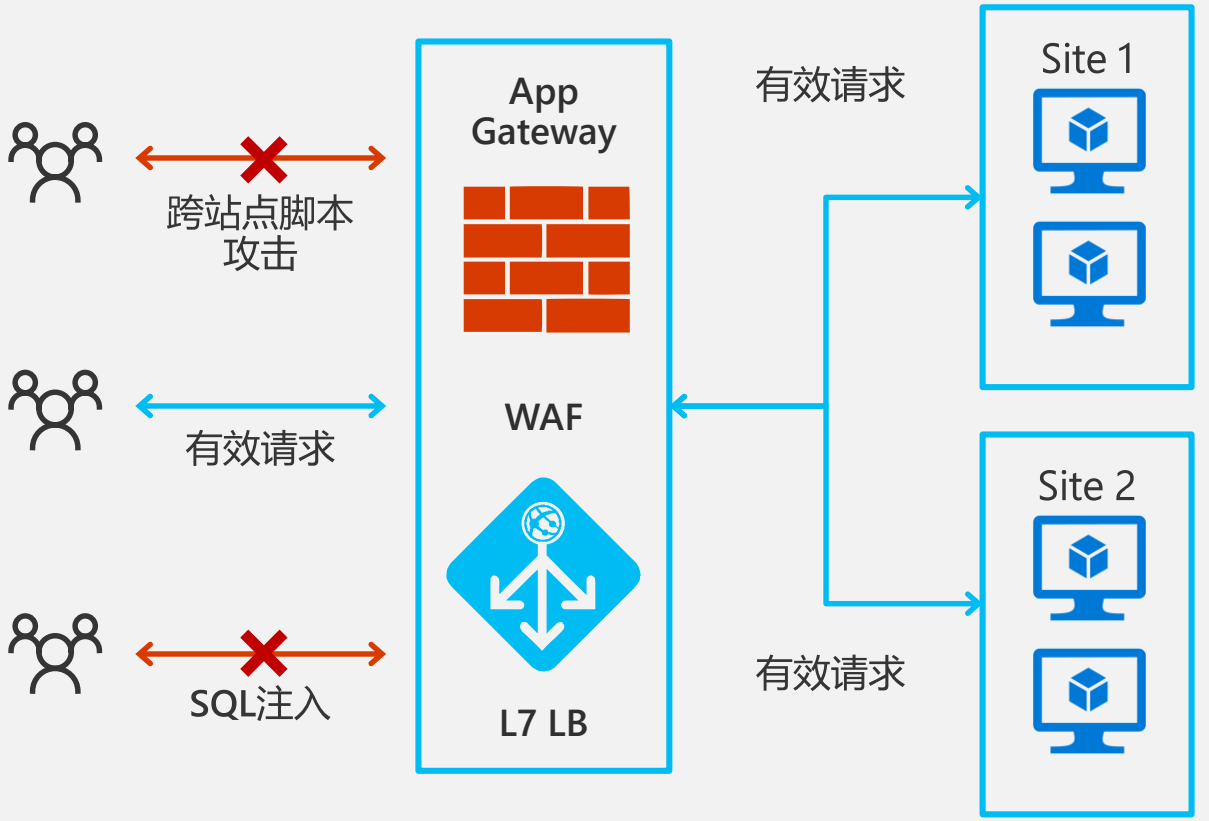


网络安全加固

- 网络安全组
- Azure 防火墙
- Web应用程序防火墙
- 远程访问和跨界连接
- 外围网络架构
- Azure DDoS防护
- 总结与补充

Web应用程序防火墙（WAF）

Azure防火墙为非HTTP/S协议（例如 RDP\SSH\FTP协议）提供入站保护，为所有端口和协议提供出站网络级别的保护；如果用户需要为HTTP/S协议提供入站保护，需要使用Web应用程序防火墙（WAF）



为应用程序提供防御跨站点脚本和SQL注入等常见攻击

WAF 与应用程序网关集成，使应用程序的安全性得到增强

与Azure安全中心集成

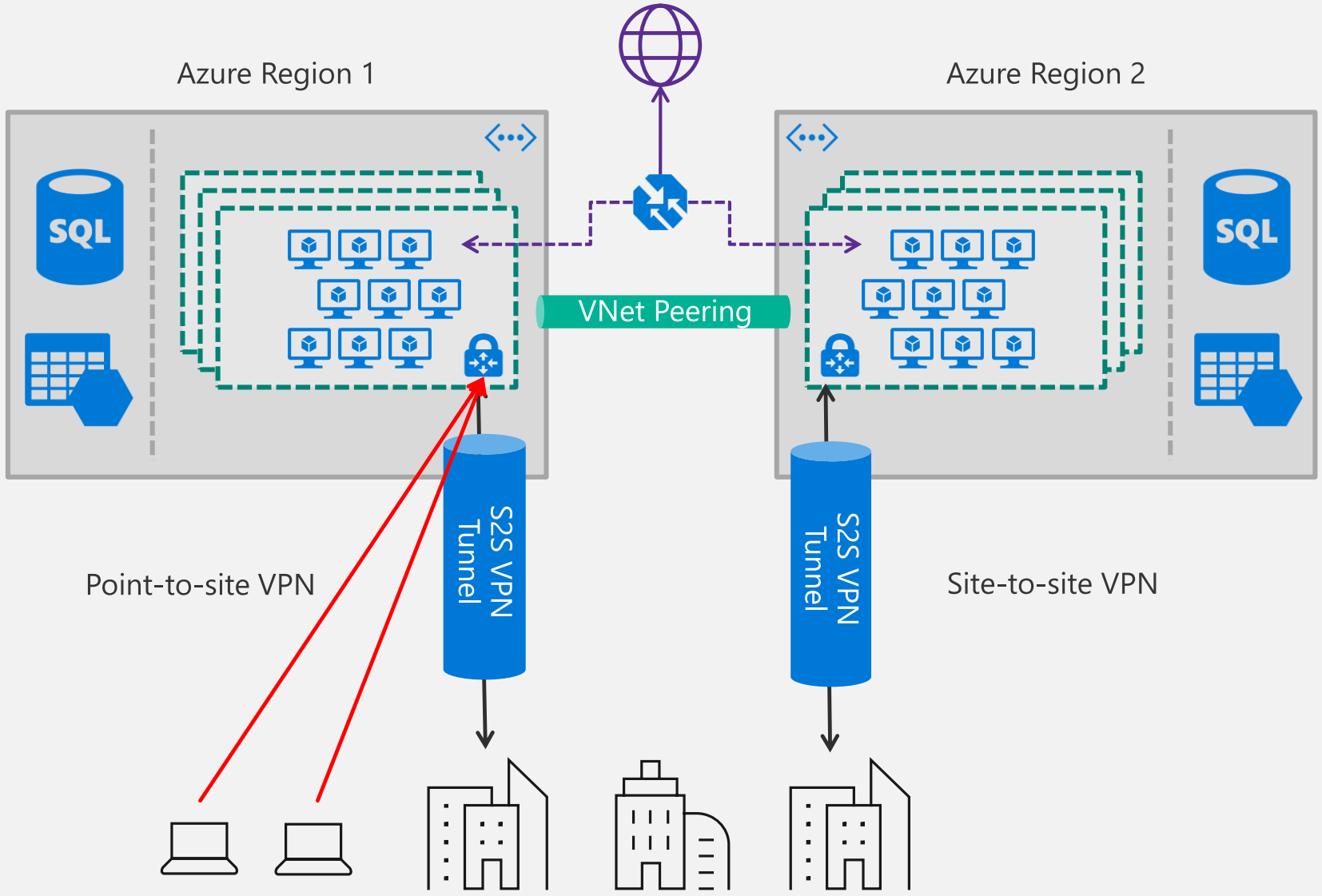
使用Azure Monitor进行实时日志记录

平台管理，可扩展和高可用性

网络安全加固

- 网络安全组
- Azure 防火墙
- Web应用程序防火墙
- 远程访问和跨界连接
- 外围网络架构
- Azure DDoS防护
- 总结与补充

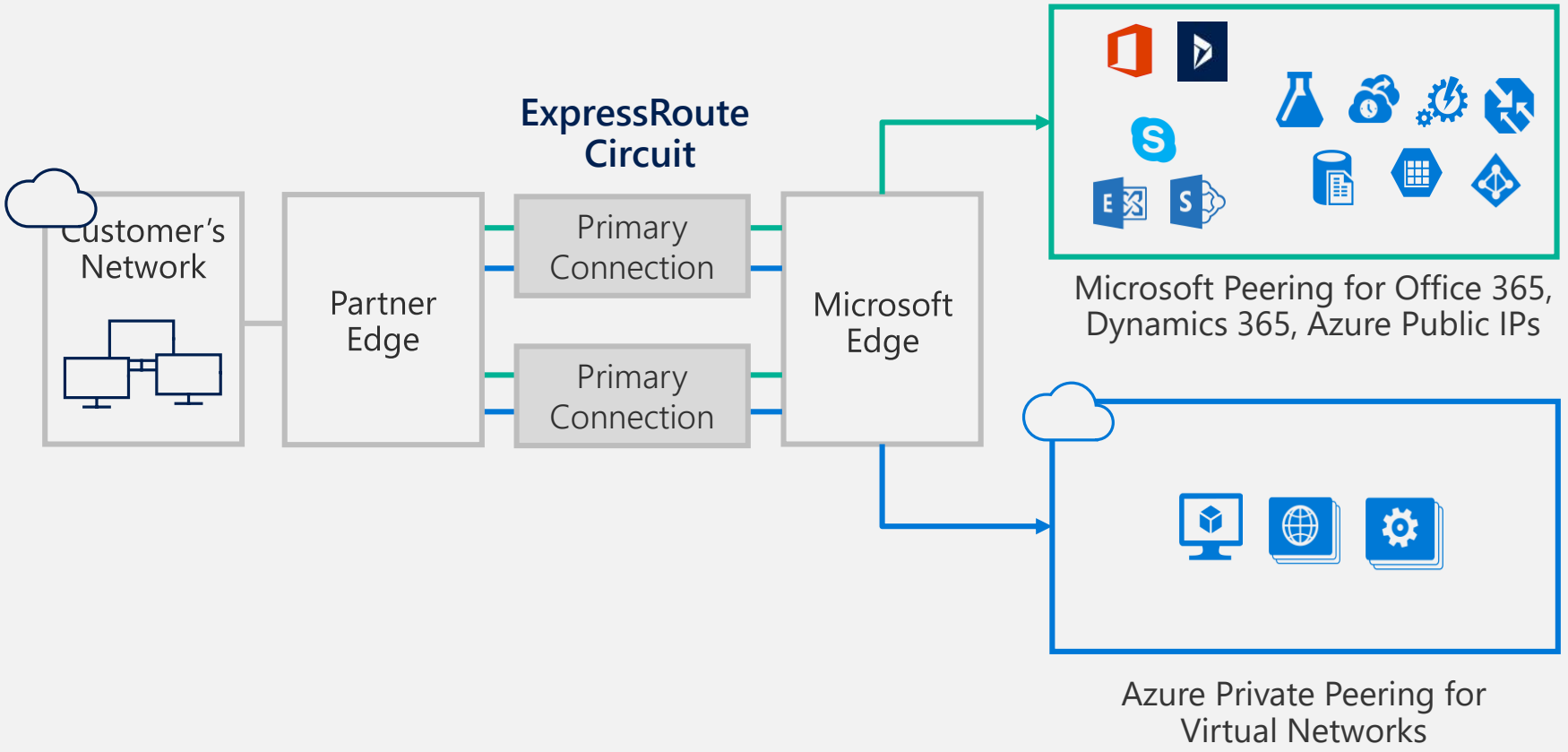
远程访问和跨界连接 – VNet Peering & VPN



远程访问和跨界连接 – ExpressRoute

ExpressRoute 连接不会通过公共Internet；具有更高的可靠性、更快的速度、更低的延迟以及更高的安全性。

用户通过从ISP提供的现有WAN网络直接连接到Azure，从而建立与Azure云的私人光纤连接。



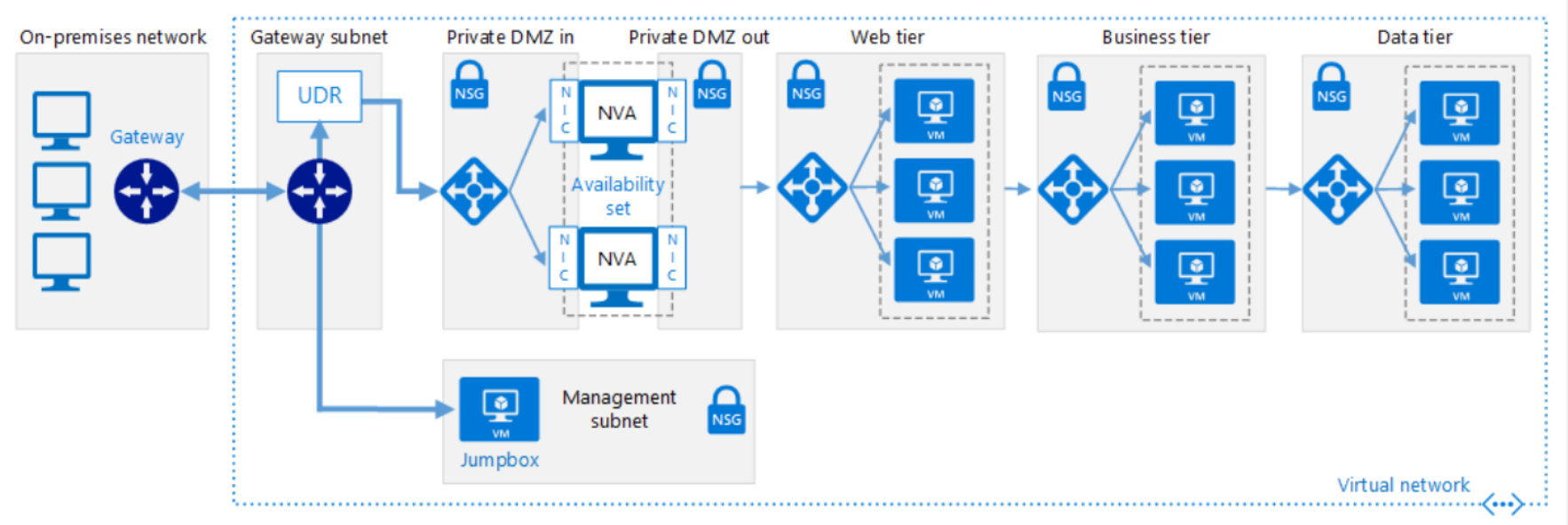
网络安全加固

- 网络安全组
- Azure 防火墙
- Web应用程序防火墙
- 远程访问和跨界连接
- 外围网络架构
- Azure DDoS防护
- 总结与补充

外围网络架构 – Azure与本地之间

本地网络与 Azure 虚拟网络 (VNet) 之间实现一个 DMZ（也称为外围网络）

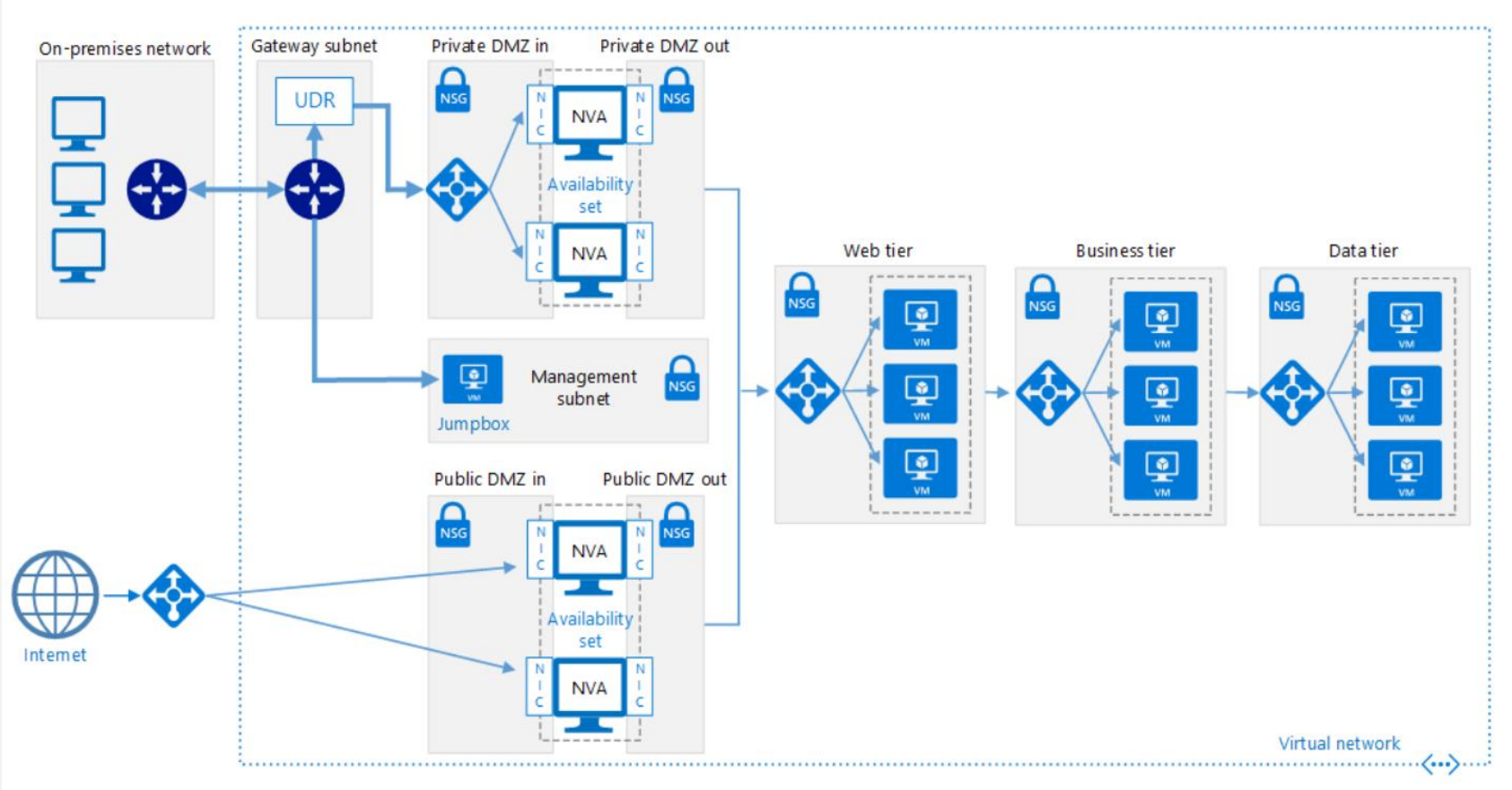
DMZ 包括**防火墙**和**数据包检查**等实现安全功能的**网络虚拟设备 (NVA)**。 来自 VNet 的所有传出流量都通过本地网络强制隧道传输到 Internet，以便可以进行审核。



外围网络架构 – Azure与Internet之间

此参考体系结构扩展了在Azure 和本地数据中心之间实现外围网络中所述的体系结构。

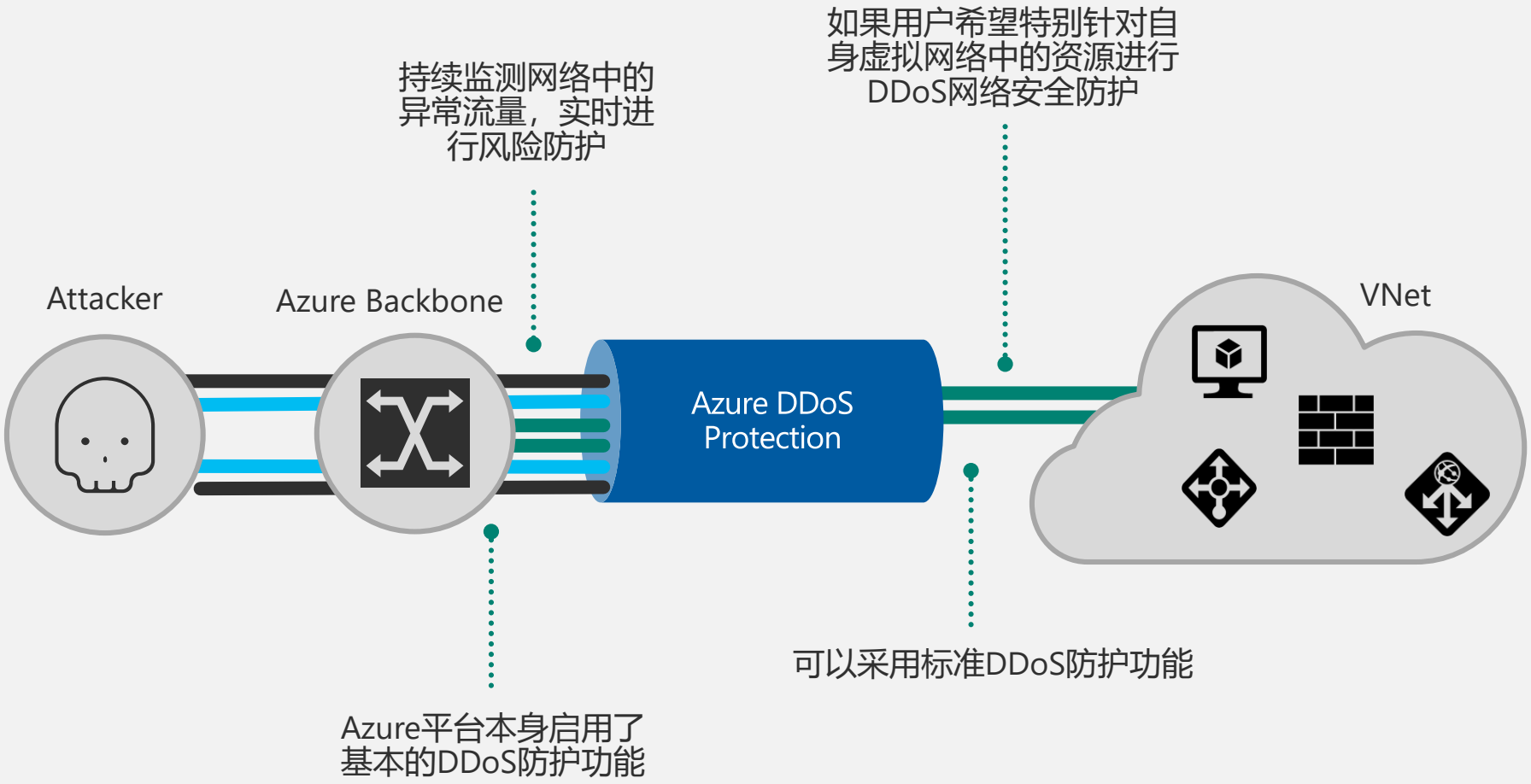
添加了一个用于处理 Internet 流量的公共外围网络，以及一个用于处理来自本地网络的流量的专用外围网络。



网络安全加固

- 网络安全组
- Azure防火墙
- Web应用程序防火墙
- 远程访问和跨界连接
- 外围网络架构
- Azure DDoS防护
- 总结与补充

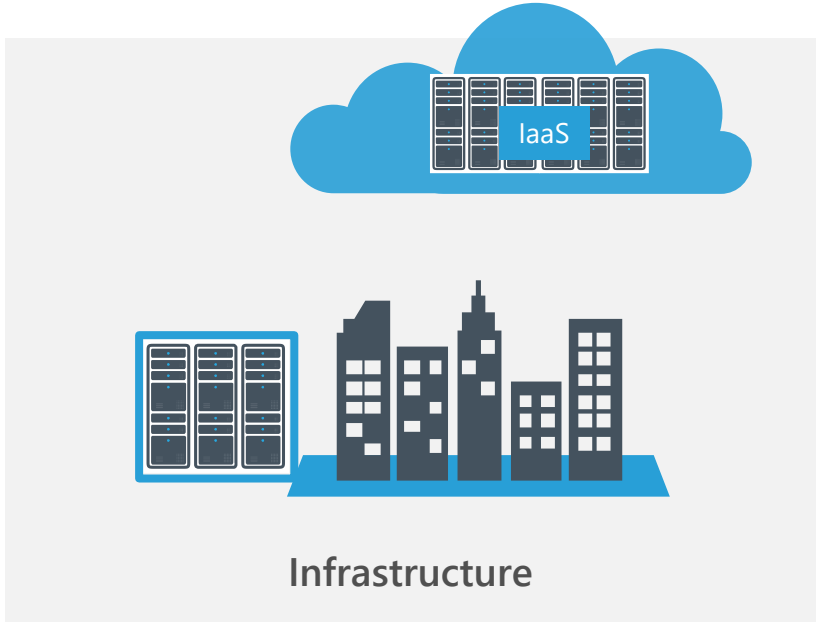
Azure DDOS防护



总结与补充

安全防护位置	边界	连接方式	安全措施
Intra-VNet	子网/网卡	VNet内部路由	NSG/ASG
Inter-VNet	虚拟网络	VNet Peering	Azure防火墙
Container pods	Container pods	Azure内部路由	Kubernetes Policies
PaaS 服务	PaaS服务账户	服务终结点	服务终结点策略/Azure防火墙FQDN筛选
与Internet交互位置	应用程序边界	Internet连接	应用程序防火墙（WAF）/DDoS防护

虚拟机的安全加固



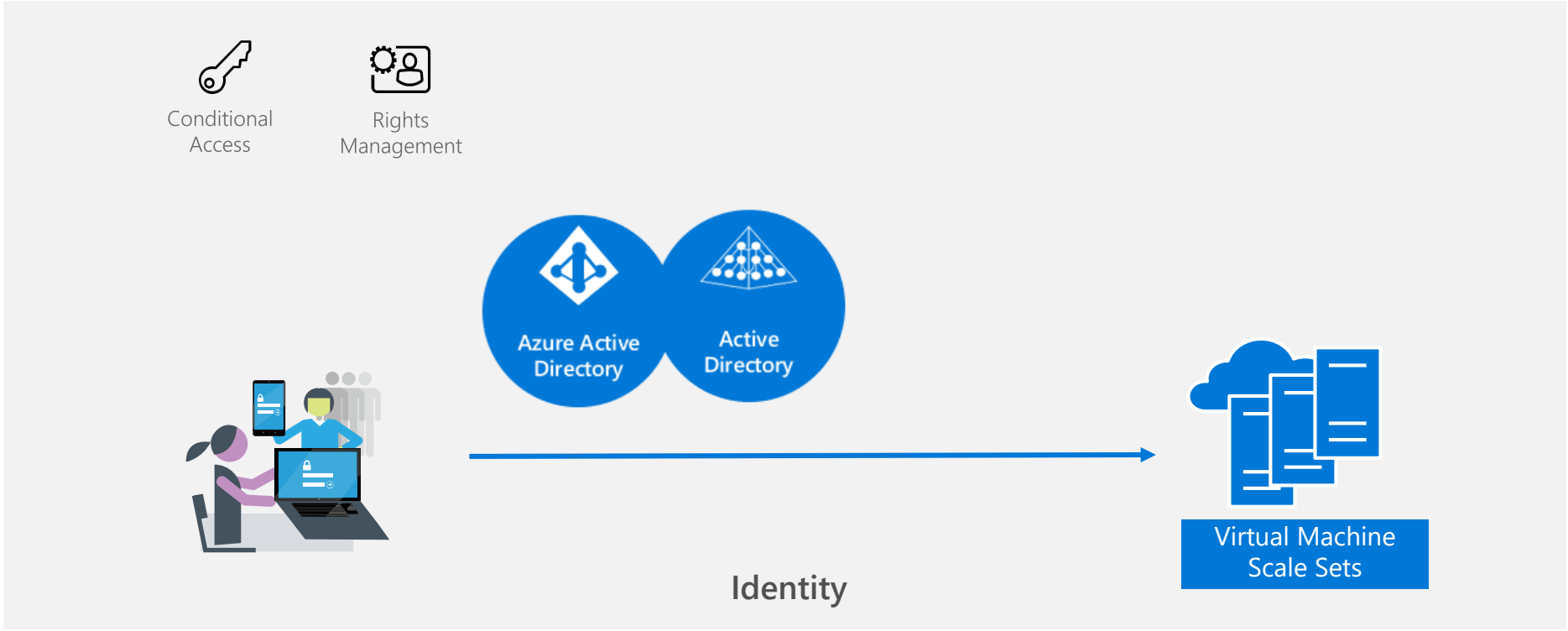
Linux虚拟机 – 开启SELinux、AppArmor等功能保护重要文件

Linux虚拟机 – 用户登录通知

Linux虚拟机 – 安全审计

- 不要使用root权限运行Web应用程序，或直接禁止root账号登录虚拟机
- 增加密码的复杂度
- 修改SSH/RDP端口为非默认端口
- 使用证书登录
- 限制IP登录
- 在虚拟机内部部署防火墙或第三方防护工具，设置服务允许拒绝规则等，防止非法的访问。在Linux上，可以通过tcp_wrappers等实现
- 根据最少服务原则，在安装配置系统时，安装应用需要的最少的包，开启最少的服务
- 通过跳板机（Jumpbox）进行内部访问，特别是数据库和重要的业务服务器
- 及时打上重要的补丁，防止应用程序被漏洞利用入侵

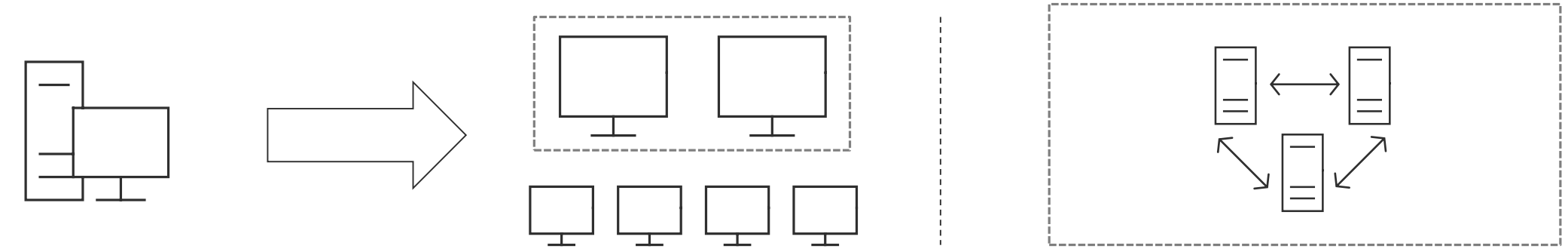
通过身份验证和访问控制保护VM



- 确保只有授权用户才能设置新 VM 以及访问 VM
- 与Azure AD 身份验证集成，降低人为引起的安全风险

使用多个 VM 提高可用性

- 在系统架构设计上，推荐将不同功能放置在不同的虚拟机上
- 按功能对虚拟机划分安全组，并设置相应的访问控制规则
- 使用可用性集或可用性区域，获得更好的可用性

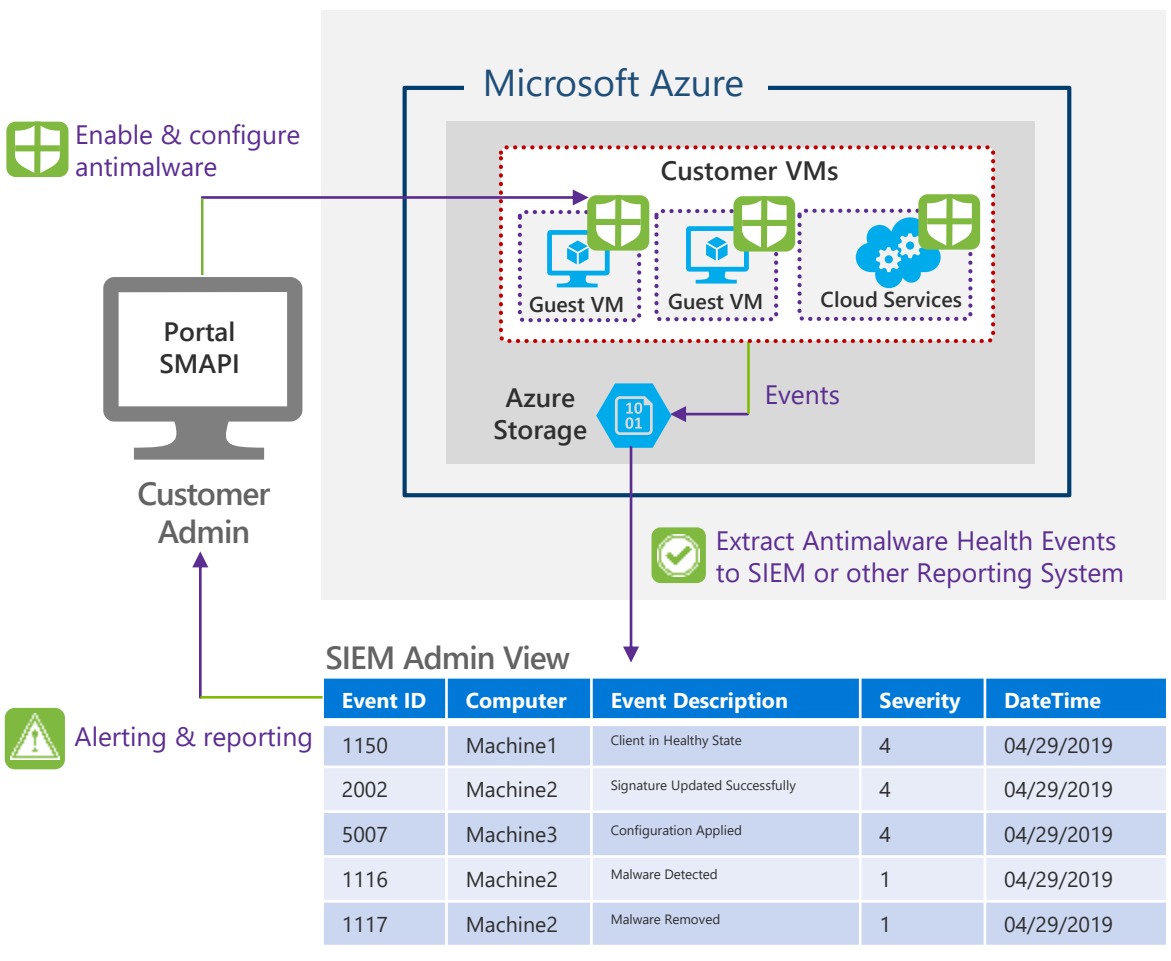


SINGLE VM

AVAILABILITY SETS

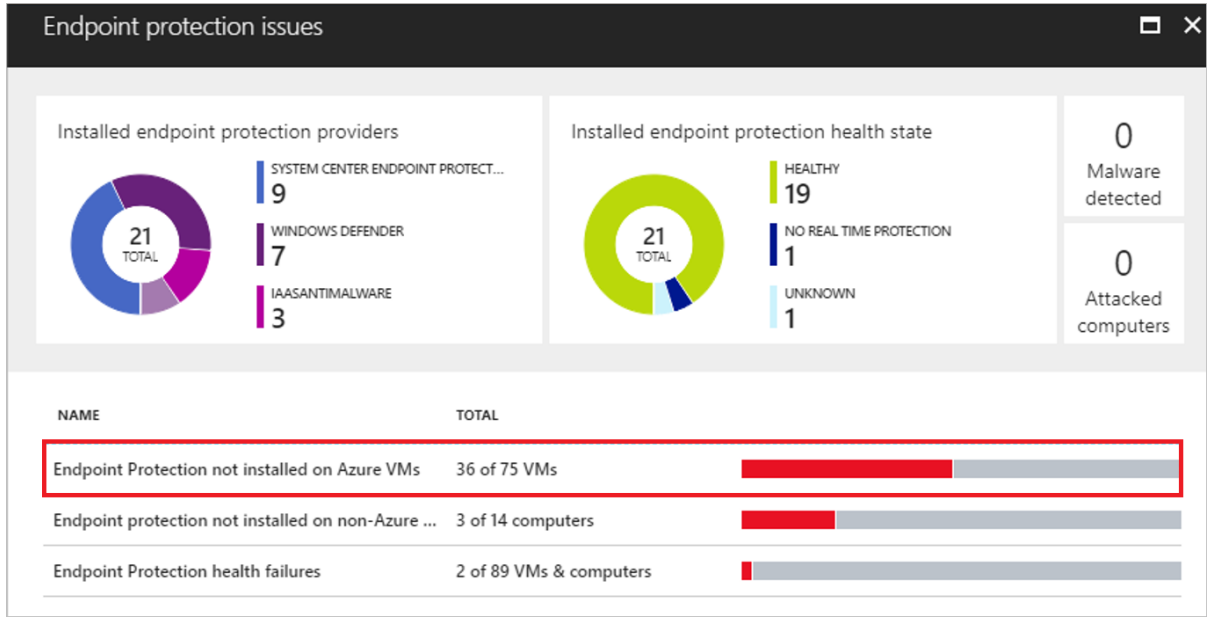
AVAILABILITY ZONES

防范恶意软件



SIEM Admin View

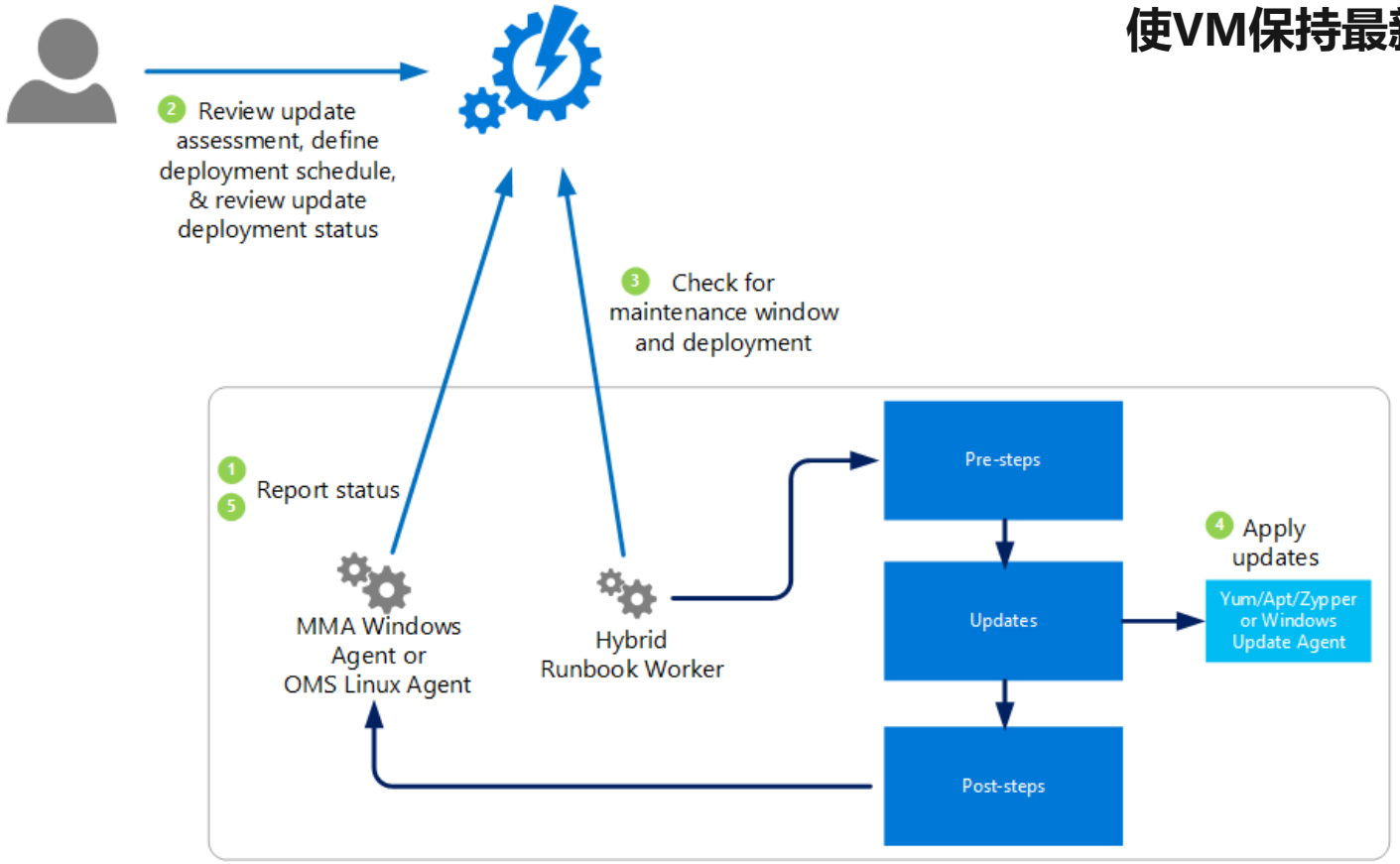
Event ID	Computer	Event Description	Severity	DateTime
1150	Machine1	Client in Healthy State	4	04/29/2019
2002	Machine2	Signature Updated Successfully	4	04/29/2019
5007	Machine3	Configuration Applied	4	04/29/2019
1116	Machine2	Malware Detected	1	04/29/2019
1117	Machine2	Malware Removed	1	04/29/2019



安装 Microsoft 反恶意软件或 Microsoft 合作伙伴的终结点保护解决方案（Trend Micro、Symantec、McAfee、Windows Defender 和 System Center Endpoint Protection）

Microsoft 反恶意软件和合作伙伴解决方案可与Azure 安全中心集成，以方便部署和内置检测（警报和事件）。

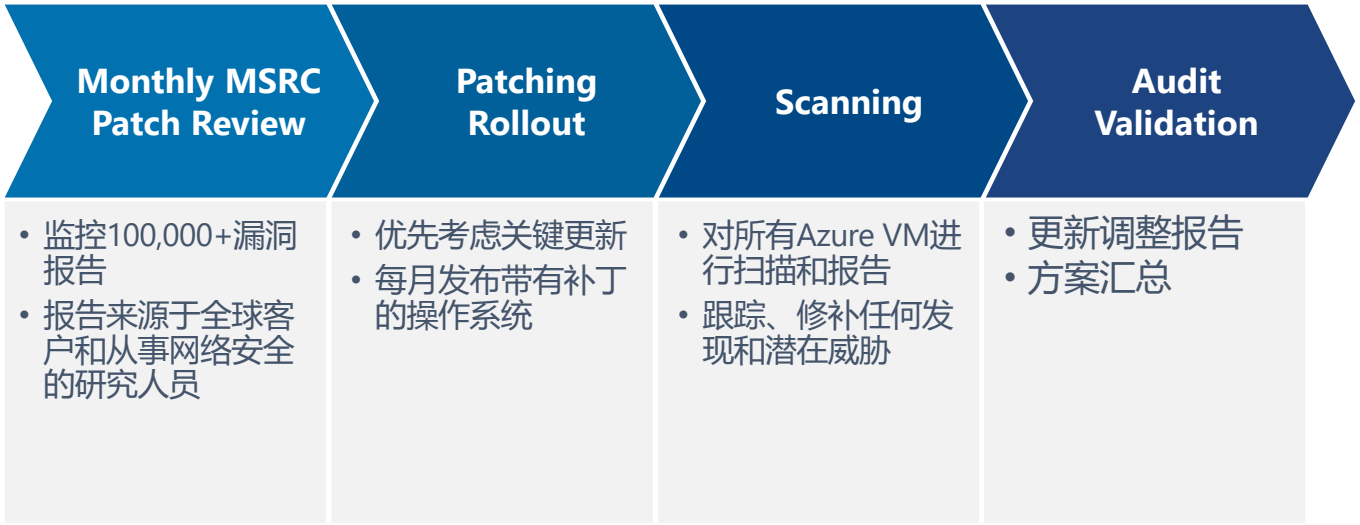
管理VM更新



使VM保持最新——由更新管理托管的计算机使用以下配置执行评估和更新部署：

- 用于 Windows 或 Linux 的 Microsoft 监视代理 (MMA)
- 用于 Linux 的 PowerShell 所需状态配置 (DSC)
- 自动化混合 Runbook 辅助角色
- 适用于 Windows 计算机的 Microsoft 更新或 Windows Server 更新服务 (WSUS)
- 若使用 Windows 更新，请启用 Windows 自动更新设置

补丁管理



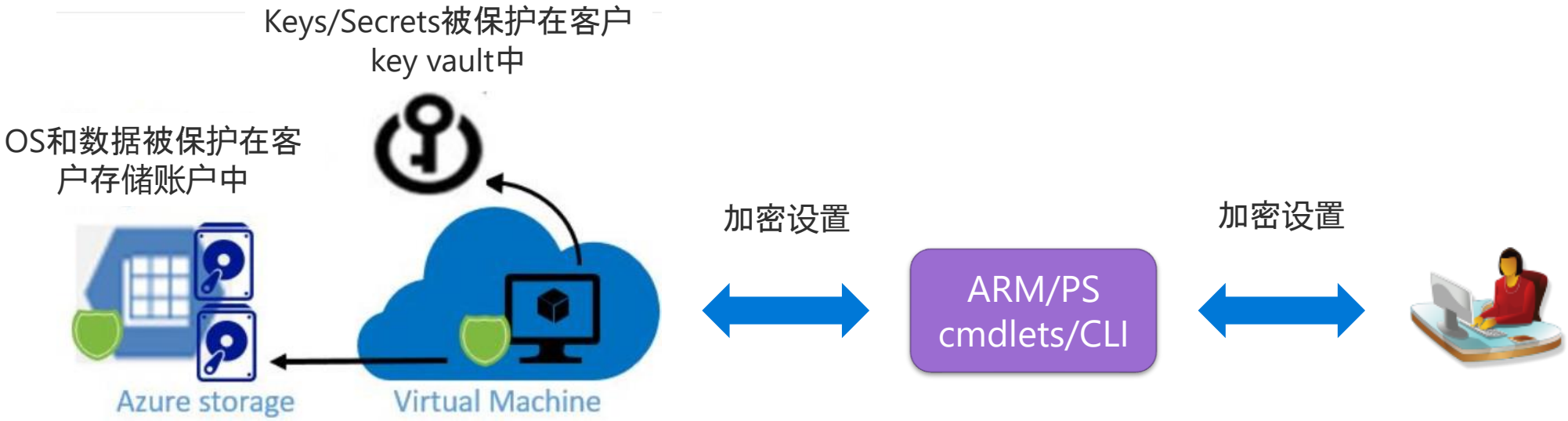
AZURE:

- 定期对平台进行更新
- 及时发布关键补丁
- 严格审查、测试所有更改

CUSTOMER:

- 针对自己的虚拟机应用类似的补丁管理策略

加密虚拟硬盘文件



- 在 VM 上启用加密
- 使用密钥加密密钥 (KEK) 来为加密密钥提供附加的安全层。 将 KEK 添加到密钥保管库。
- 为确保加密机密不会跨过区域边界，Azure 磁盘加密需要将密钥保管库和 VM 共置在同一区域。

数据保护

Azure为客户提供了强大的数据安全性

数据隔离

默认情况下，每个客户的数据与其他客户的数据逻辑隔离开来。

静态数据保护

客户可以为虚拟机和存储实现一系列加密选项。

传输中的数据保护

行业标准加密协议对在Azure组件间传输数据进行加密，默认情况下Azure也对内部传输的数据进行加密。

数据加密

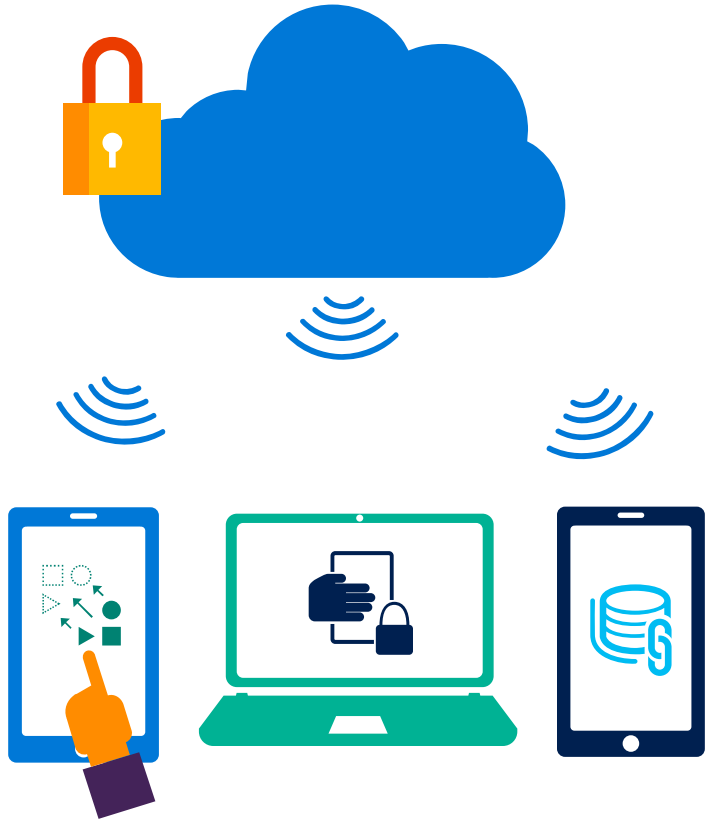
客户可以部署存储或传输中的数据加密，以确保数据的机密性和完整性。

数据冗余

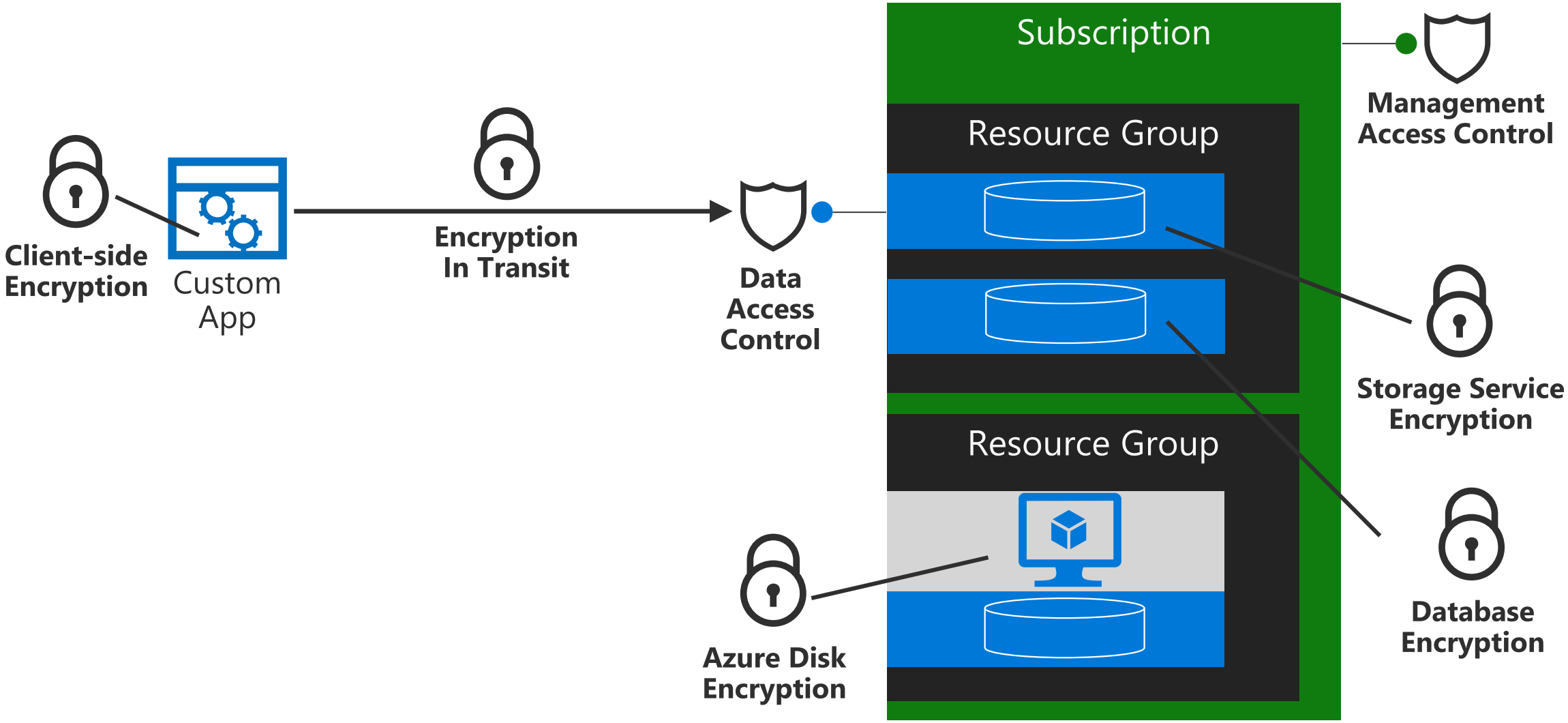
客户有多种选择进行数据的复制，包括设置复制的数量和复制数据中心的数量和位置。

数据销毁

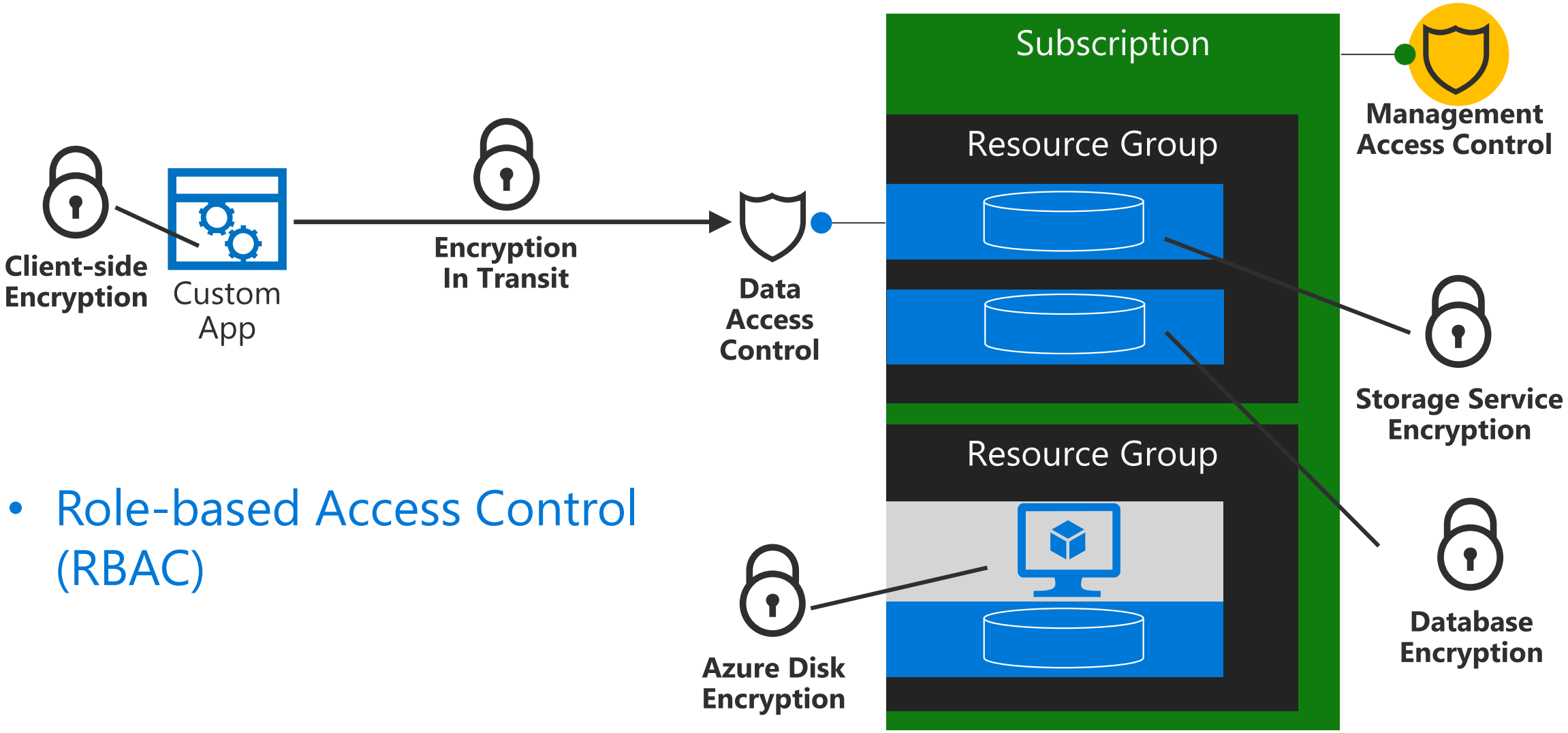
当客户删除数据或不使用Azure时，微软会按照相关数据销毁步骤来让以前的数据无法再次被访问和使用



Azure数据安全

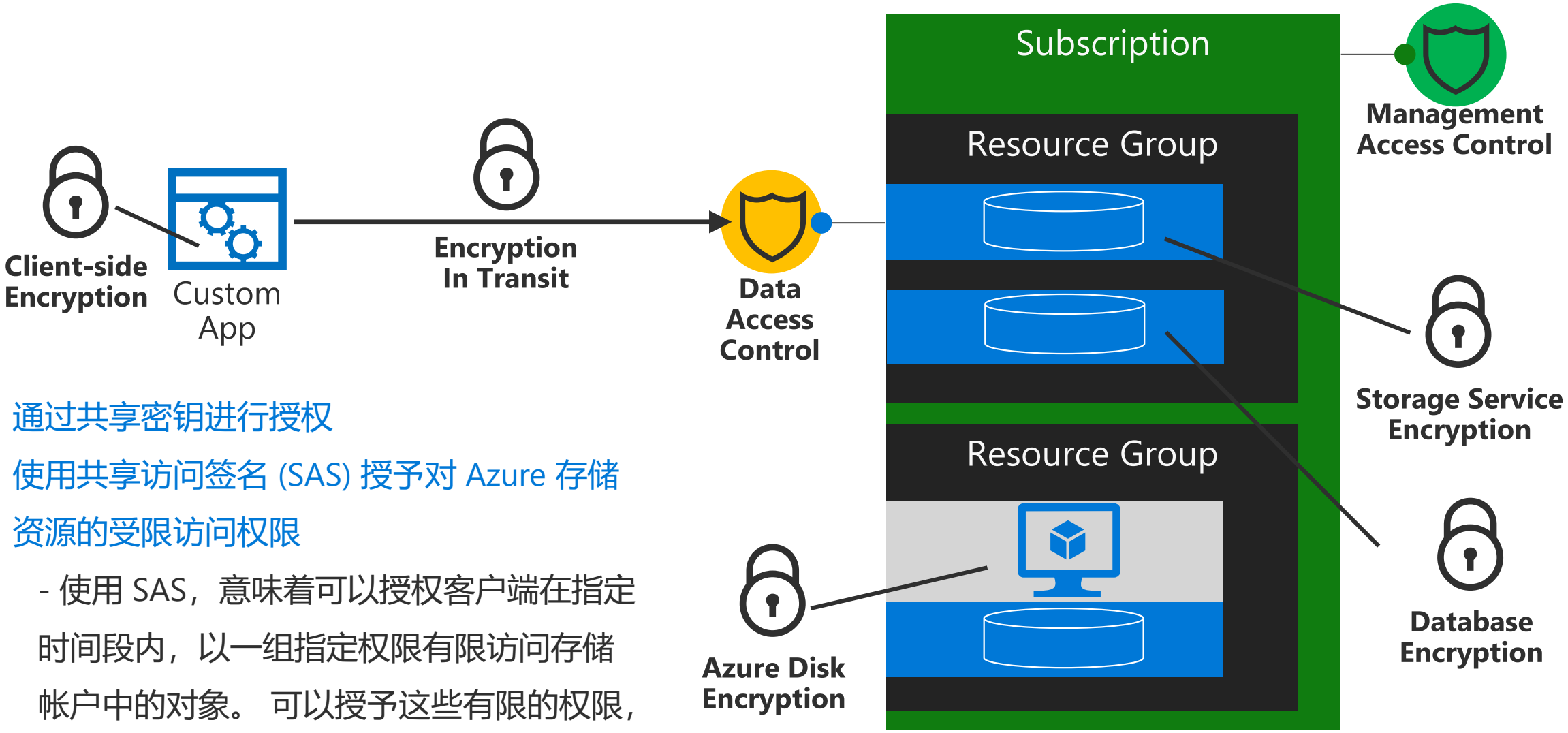

Subscription
Resource Group
Resource Group
Management Access Control
Client-side Encryption
Custom App
Encryption In Transit
Data Access Control
Storage Service Encryption
Azure Disk Encryption
Database Encryption

基于角色的访问控制



- Role-based Access Control (RBAC)

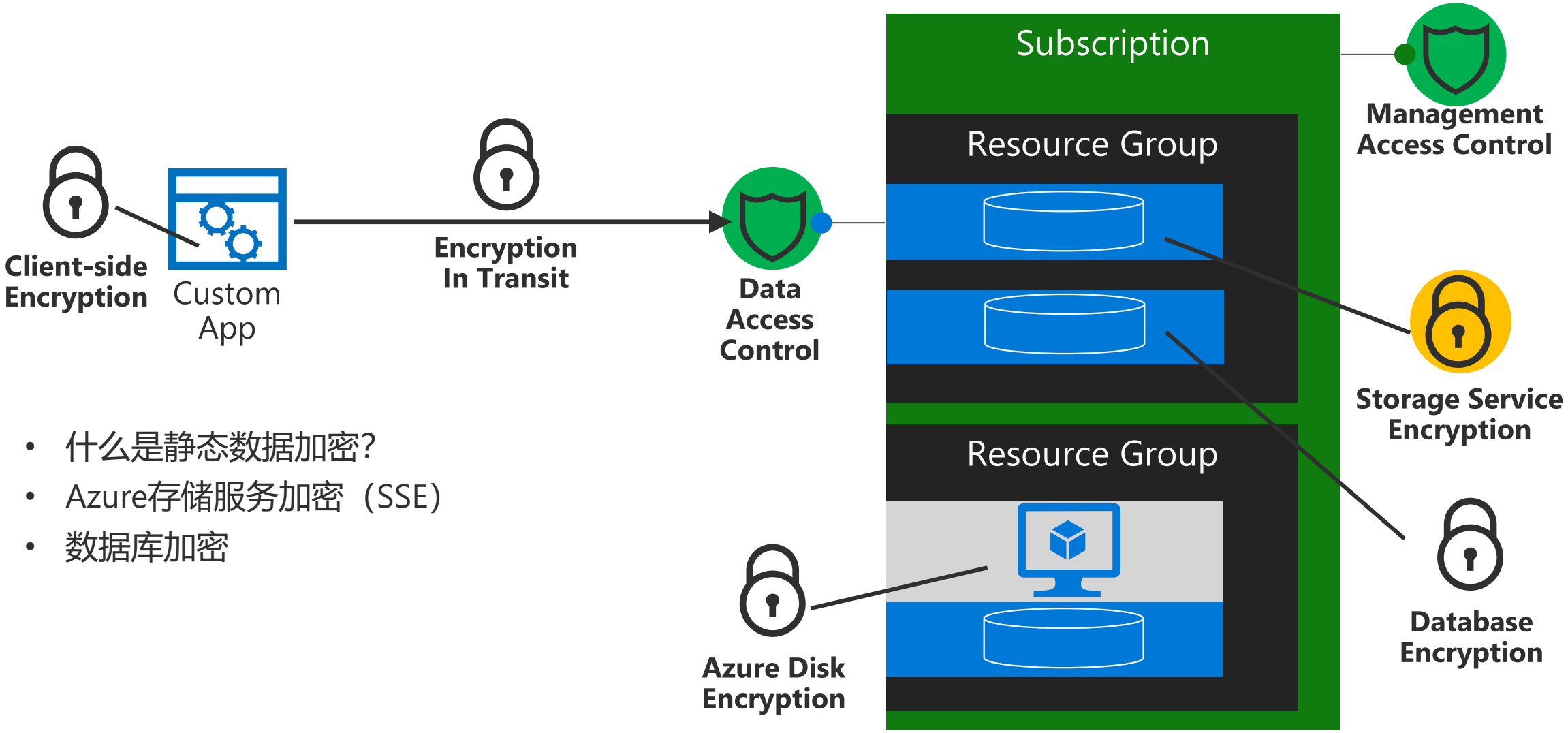
存储对象的委托访问权限



- 通过共享密钥进行授权
- 使用共享访问签名 (SAS) 授予对 Azure 存储资源的受限访问权限

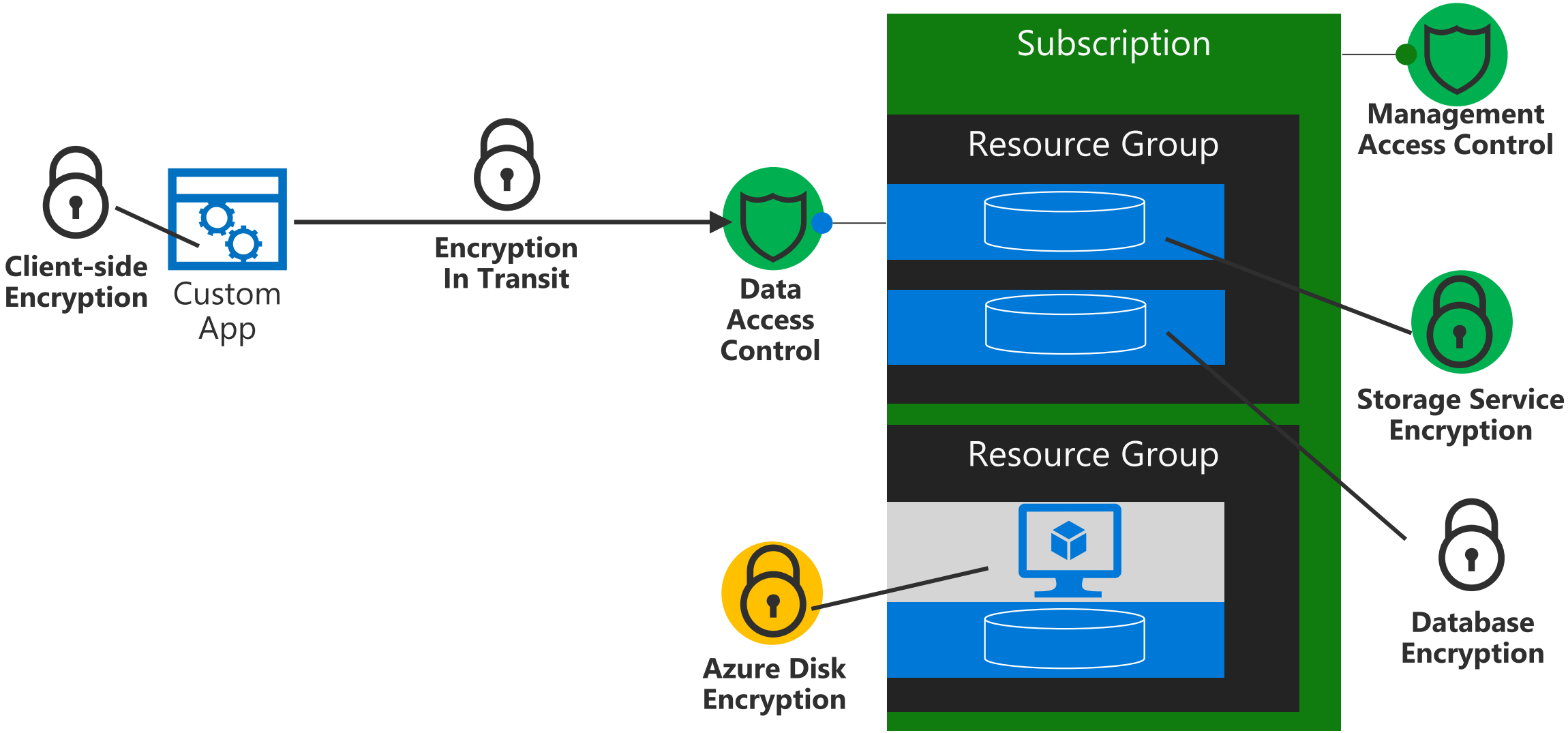
  - 使用 SAS，意味着可以授权客户端在指定时间段内，以一组指定权限有限访问存储帐户中的对象。 可以授予这些有限的权限，而不必共享帐户访问密钥。

数据加密 – 静态数据加密

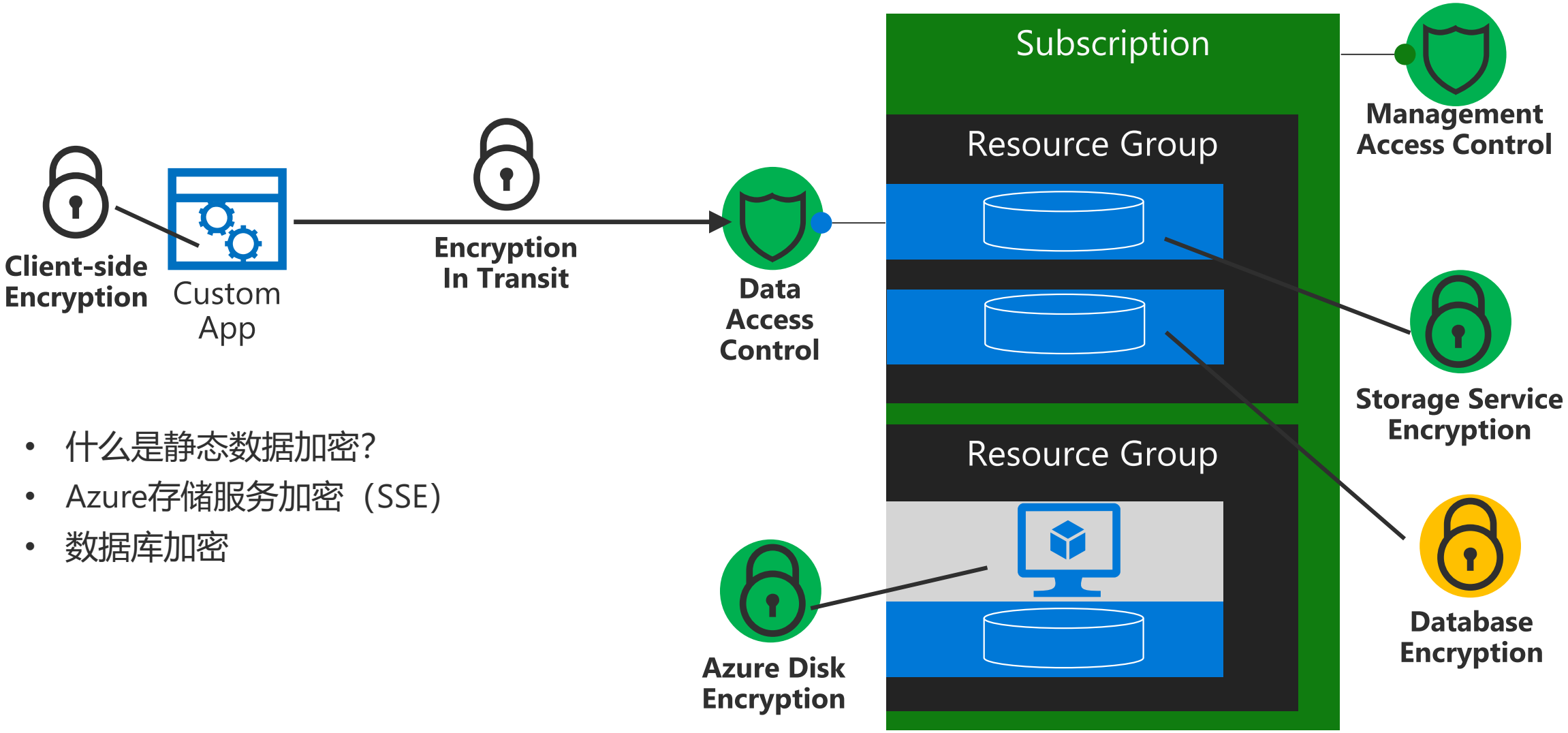


- 什么是静态数据加密?
- Azure存储服务加密（SSE）
- 数据库加密

数据加密 – 静态数据加密

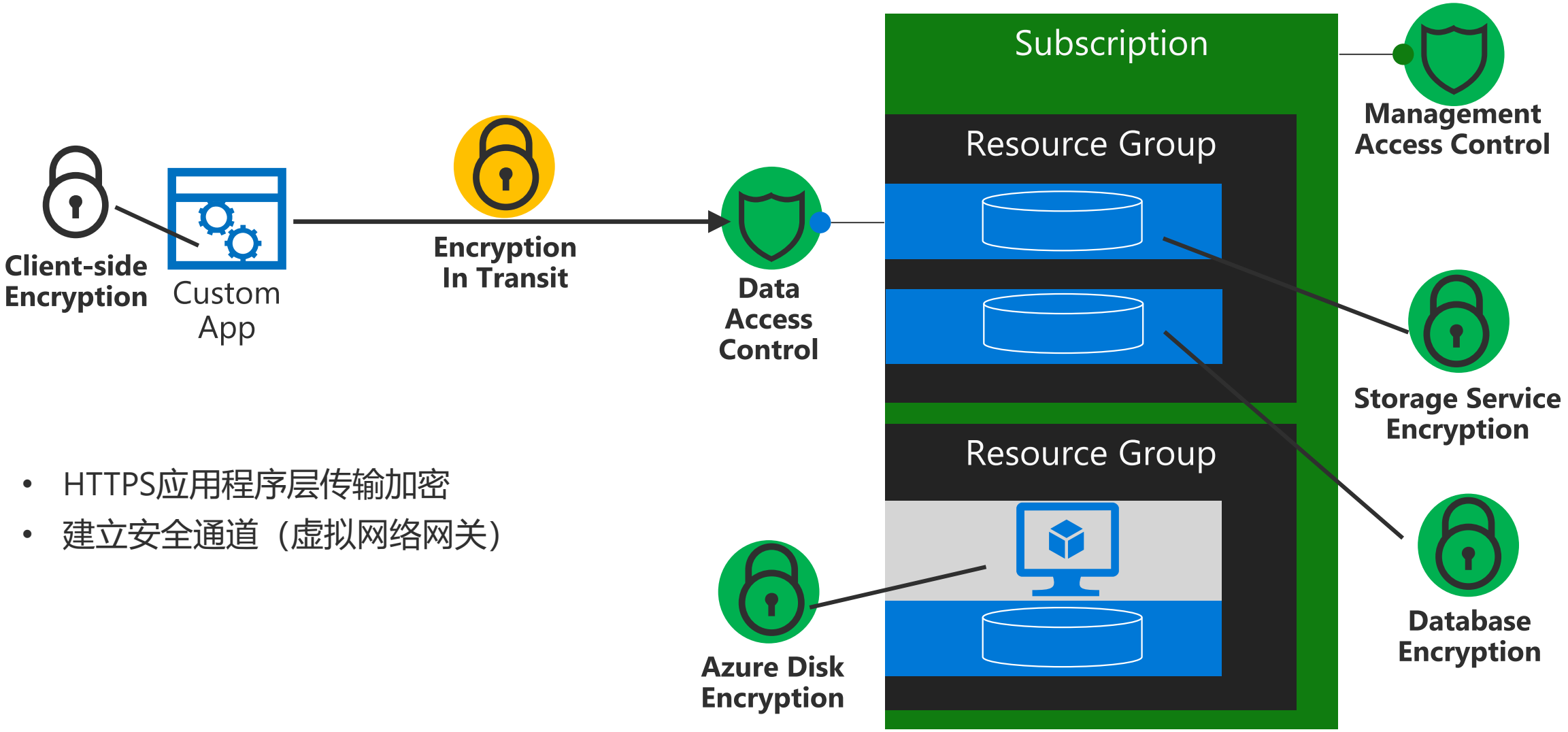

Client-side Encryption
Custom App
Encryption In Transit
Data Access Control
Subscription
Resource Group
Resource Group
Management Access Control
Storage Service Encryption
Database Encryption
Azure Disk Encryption

数据加密 – 静态数据加密



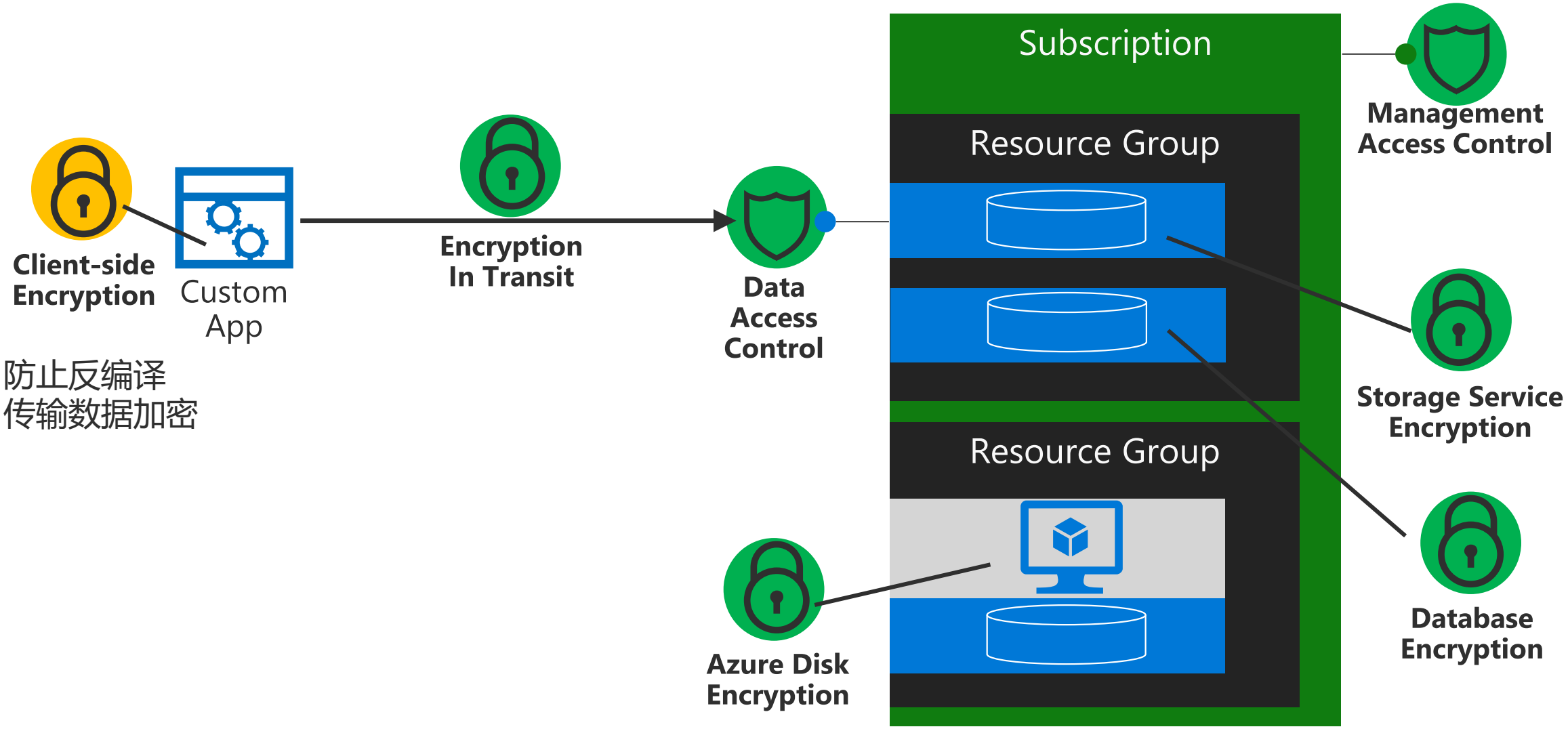
- 什么是静态数据加密?
- Azure存储服务加密（SSE）
- 数据库加密

数据加密 – 传输中加密



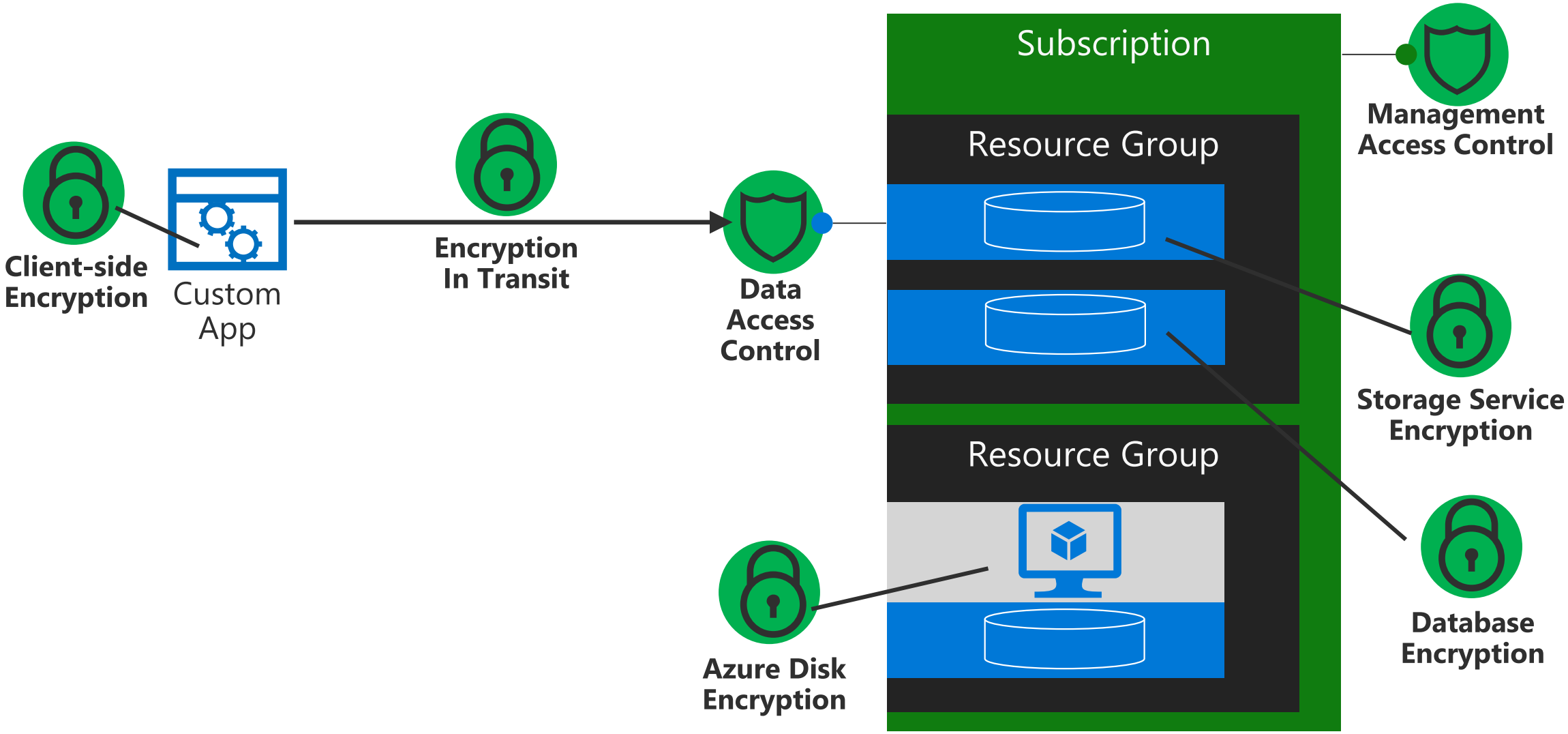
- HTTPS应用程序层传输加密
- 建立安全通道（虚拟网络网关）

数据加密 - 客户端加密



- 防止反编译
- 传输数据加密

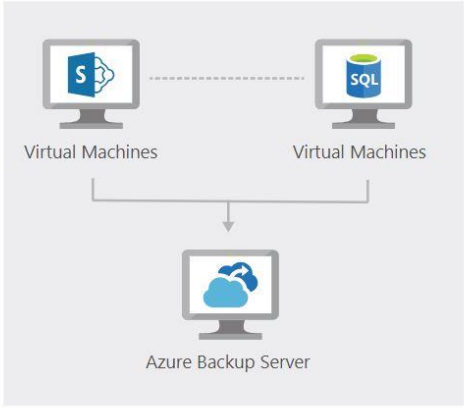
Azure数据安全

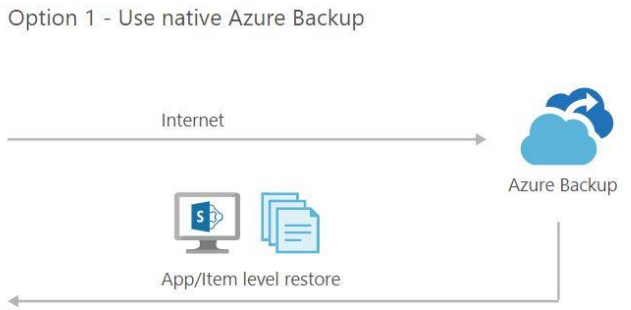

Subscription
Resource Group
Resource Group
Management Access Control
Client-side Encryption
Custom App
Encryption In Transit
Data Access Control
Storage Service Encryption
Azure Disk Encryption
Database Encryption

数据保护——备份和站点恢复

备份

- ✓ Azure 备份是基于 Azure 的服务，可用于备份（或保护）和还原 Microsoft 云端数据
- ✓ Azure 备份将现有的本地或异地备份解决方案替换为安全可靠、性价比高的云端解决方案。

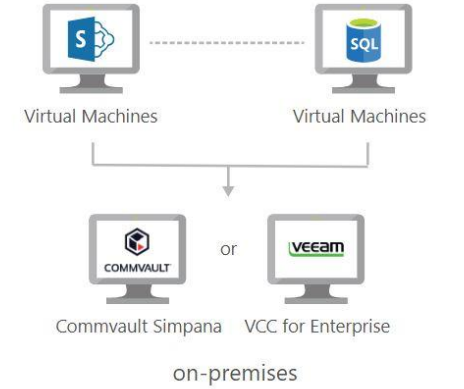


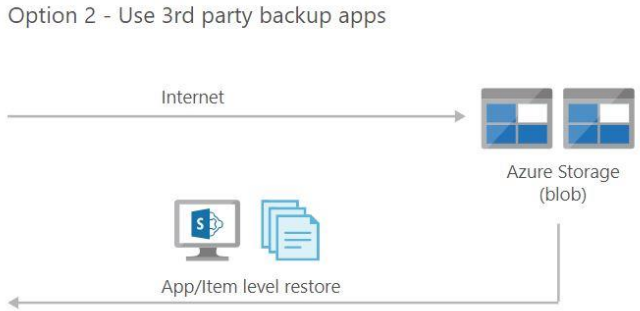


站点恢复

可以将以下内容复制到 Azure：

- ✓ VMware：可以复制运行支持的操作系统的 VMware VM
- ✓ Hyper-V：本地 Hyper-V VM，运行在支持的主机上
- ✓ 物理机：本地物理服务器，在支持的操作系统上运行 Windows 或 Linux、





Azure Key Vault 密钥保管库

- **机密管理**

  - 可以用来安全地存储令牌、密码、证书、API 密钥和其他机密，并对其访问进行严格控制

- **密钥管理**

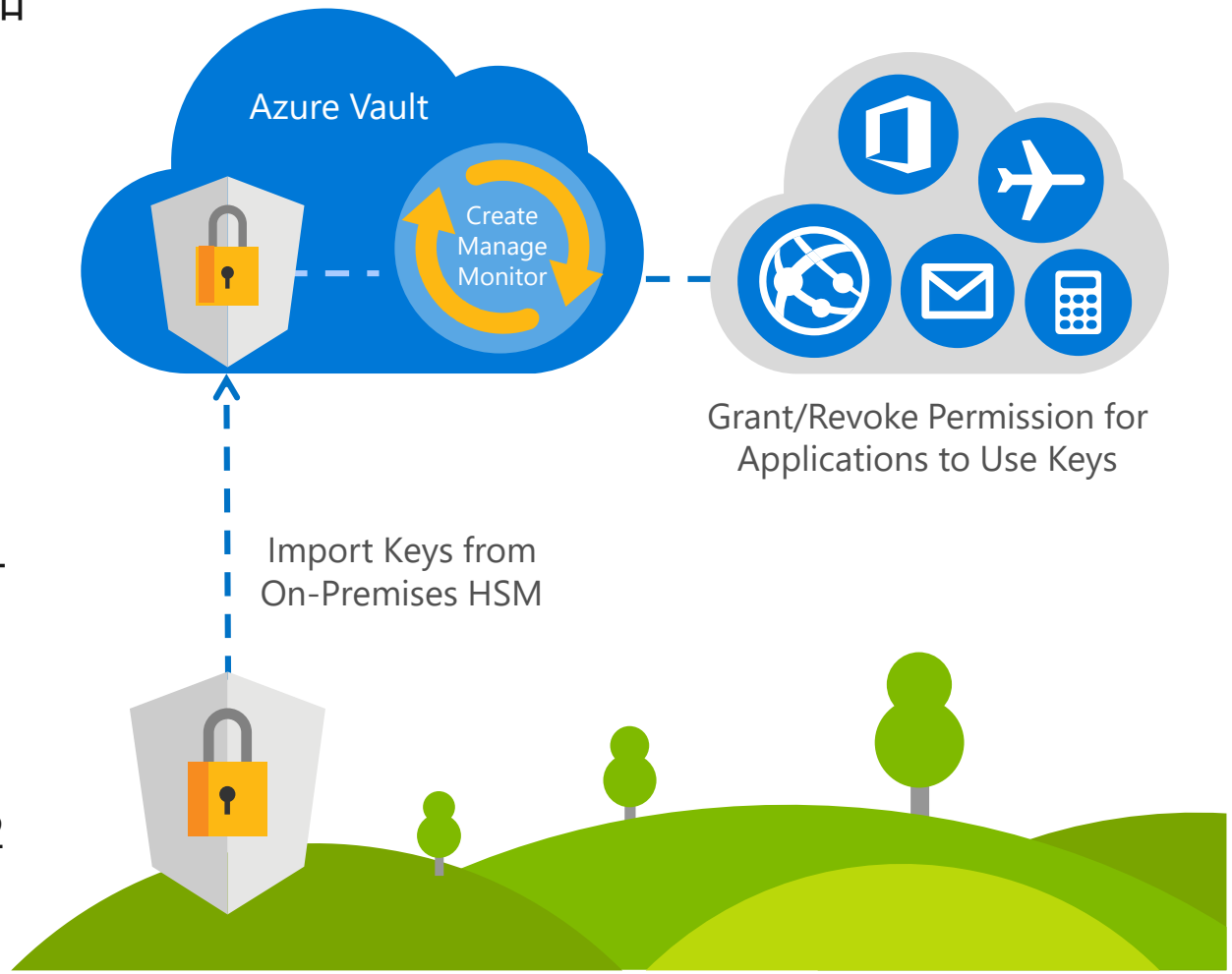
  - 可用作密钥管理解决方案。 可以通过 Azure Key Vault 轻松创建和控制用于加密数据的加密密钥。

- **证书管理**

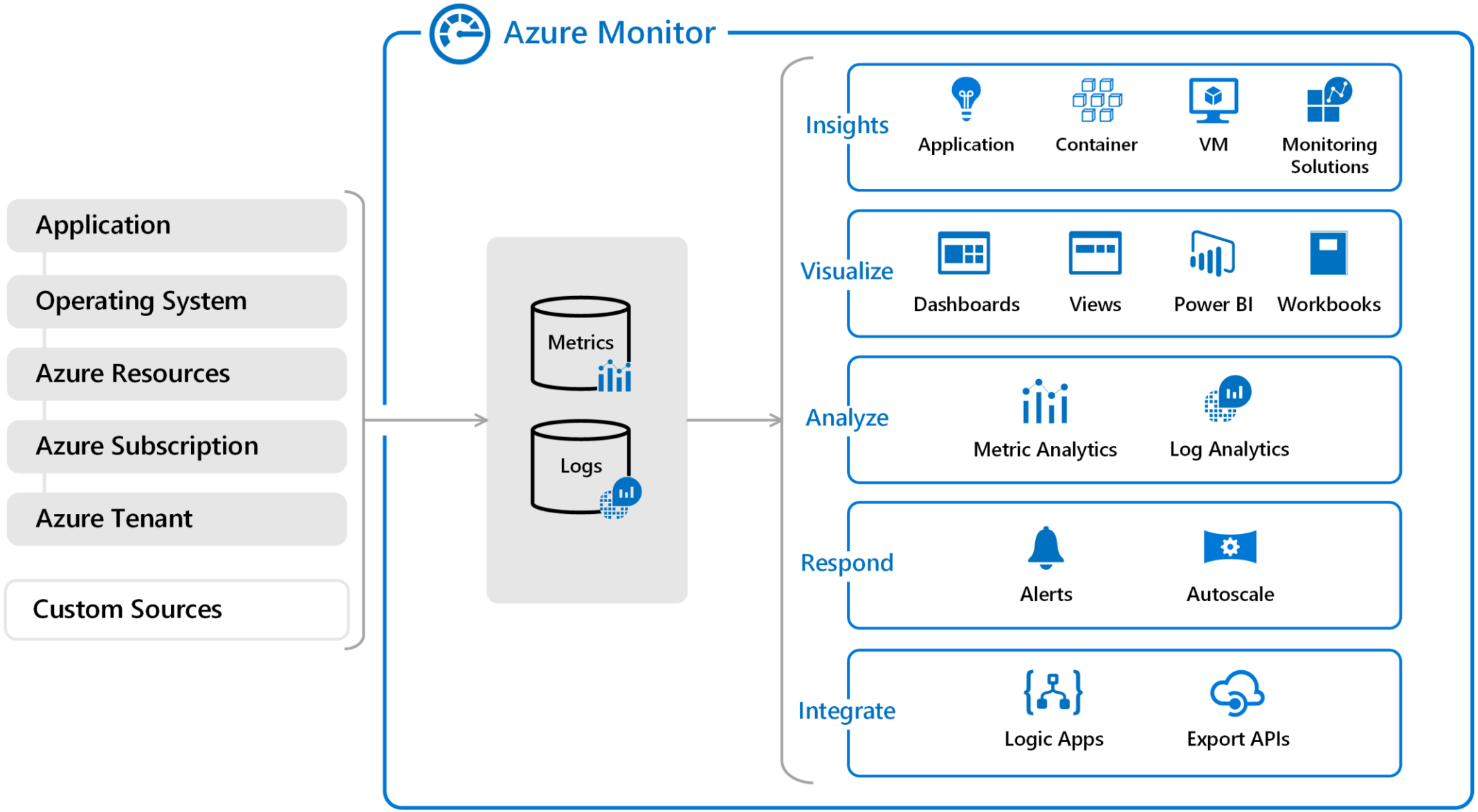
  - 可以用来轻松地预配、管理和部署公用和专用安全套接字层/传输层安全性 (SSL/TLS) 证书，这些证书可以与 Azure 以及你的内部连接资源配合使用。

- **存储由硬件安全模块提供支持的机密**

  - 这些机密和密钥可以通过软件或 FIPS 140-2 级别 2 验证 HSM 进行保护



Azure Monitor监控VM性能指标



Thanks ☺