Microsoft

Azure Zero Trust Controls: Platform Threat Vector

Authors

Doreen Galli PhD MBA

Darius Ryals

Arjuna Shunn

Contributors

Sharon Sandhu

Lucio C Tinoco

Karina Juarez (CELA)

Graham Bury

Microsoft

Introduction

This document describes how to protect data in an Azure tenant from risk sourced from the cloud service provider. Strict data protection and residency laws and regulations are becoming prevalent across the globe. Many organizations are forced to evaluate various clouds' suitability for data protection given these evolving legal and regulatory requirements. Customers want to ensure they can provide the type of data protection required by law and desired by their organization. This document focuses on zero trust principles to minimize exposure of your data to the Azure platform. For a guide to zero trust on Azure, see Zero Trust Security in Azure.

Common Customer Profiles

The following are common customer profiles that are realized in Azure and the products that enable the required protections.

Profile 1: Baseline Protection

- General Cloud Usage
- Not subject to regulatory restrictions
- Not subject to country data restrictions

Profile 2: Regulated Industry

- Banking, Finance, Insurance
- Healthcare, Life & Safety
- Minimum security requirements
- Restrictions on data access

Profile 3: Data Geographic Boundary

- Common global data regulations require data movement restrictions
- GDPR & Schrems II Ruling

Profile 4: Reduced Unauthorized Non-Customer Data Access

- Most sensitive data
- Government Classified
- Military
- Zero Trust: Platform Threat Vector

Each of these profiles builds upon the prior to support a further refinement of mitigating risk of data leakage or loss, based on specific customer need and risk appetite.

Profile 1. Baseline protection: This profile covers basic enterprise cloud usage and the recommended steps to protect your data.

Profile 2. Regulated industry: This profile is applicable to customers in regulated industries such as healthcare, finance or otherwise subject to regulatory controls and industry requirements.

Profile 3. Data boundary: This profile is applicable to customers with data residency requirements such as data must remain within a particular geographic boundary.

Profile 4. Reduce unauthorized non-customer access: This profile is applicable to customers wishing to reduce data access by the cloud provider. This profile shares two architecture varieties leveraging confidential computing.

Each of these customer profiles is evaluated in terms of the customer enabled protections that are available as depicted in Table 1. For descriptions of the protections built into Azure that do not require customer enablement included in this document, see the Appendix of Platform Protections. A depiction of these platform capabilities as applicable to the use cases is represented in Table 2.

Table 1: Customer Enabled Protections

Protection	Baseline Protection	Regulated Industry	Data Boundary	Reduce Non-Customer Access
Audit of Access Permission Granted	O	X	X	X
Confidential Inferencing Protections		O	O	O
Customer Data Geographic Protection			X	
CMK Encryption at Rest (Customer Managed Key)	O	X	X	X
Ensure Location of Data Access			X	
Hardware as the Root of Trust				X
Isolated Computing Environment		O	O	X
Isolate Enterprise Components	O	X	X	X
Manage Enterprise Access (RBAC)	X	X	X	X
Trusted Execution Environment				X
Protect Inbound and Outbound Network Flows	X	X	X	X
Protection from All Operators				O
Protection from Possession of hardware				X
Protection from Malicious Service				X
Protection from Physical Access				X

Protection While in Transit (Internet)	*X*	*X*	*X*	*X*
Reduce Risk of Data Exfiltration/Infiltration	*X*	*X*	*X*	*X*
Sensitive Application Logic Protections				*X*
Legend	**X=required**	**0=optional**		

Table 2: Platform Provided Protections

Protection	Baseline Protection	Regulated Industry	Data Boundary	Reduce non-Customer Access
Accountability for Platform Changes	*X*	*X*	*X*	*X*
Breach Mitigation	*X*	*X*	*X*	*X*
Customer Identity Geographic Protection	*X*	*X*	*X*	*X*
Encryption at Rest	*X*	*X*	*X*	*X*
Impersonation Protection User Level	*X*	*X*	*X*	*X*
Hypervisor Isolation	*X*	*X*	*X*	*X*

Platform Encryption at Rest and in Transit	X	X	X	X
Protection from Corp Identity Compromise	X	X	X	X
Protection from Known Vulnerabilities	X	X	X	X
Protection from Malware	X	X	X	X
Protection from Mistaken Deletes	X	X	X	X
Protection from Malicious Platform Changes	X	X	X	X

Profile 1: Baseline Protection

The first profile applies to most customers using the cloud. Many customers are managing the technology of their enterprise but are not subject to strict regulatory requirements. The customers primarily want to protect their data from ransomware, internet attacks, phishing attacks, data exfiltration, and malware and viruses while maintaining and evolving secure posture. To achieve this solution the following is the reference customer product stack that enables the desired protections.

Platform Protections

All platform protections described in the Appendix and in Table 2 apply to the baseline protection case.

Customer Product stack

The following is the customer product stack that the customer must deploy/enable to realize this scenario.

- Azure Virtual Network: Add security layers to the virtual machines networks that host the application therefore protecting inbound and outbound network flows.
- Virtual Network Service Tags: If your solution is leveraging a VPN over the internet, then it is critical to leverage service tags in the appropriate source or destination field. This will achieve

additional protection while in transit (Internet-based solutions) and network isolation to only authorized callers.

- Network Security Groups: A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. Denial of outbound network traffic from Azure resources provides isolation of enterprise components to limit data leakage from key services like HR systems to other enterprise systems.
- Azure Firewall: Azure Firewall Standard provides L3-L7 filtering and threat intelligence feeds directly from Microsoft cyber-security teams. Threat intelligence-based filtering can alert and deny traffic to and from known malicious IP addresses and domains which are updated in real time to protect against new and emerging attacks. Denying traffic and alerting on anomalous traffic, Azure Firewall reduces the risk of data exfiltration and infiltration.
- Encryption At Rest with Azure Key Vault: By using Azure Key Vault, the customer can trust that keys are stored in a hardware security module (HSM) and are securely controlled and managed.
- RBAC: Role-based access control is critical to manage your enterprise access to resources. Azure provides the capability for any enterprise to exercise separation of concerns and separation of controls. This ensures that only the right individuals have the desired access to your overall solution via Azure Active Directory (AAD). For customers with hybrid environments, leverage the AAD guide to ensure effective hybrid identity solutions (AAD B2B and B2C).

Profile 2: Cloud Enterprise Usage for Regulated Industry

Industries managing sensitive data need to meet heightened regulatory requirements for the protection of data. Azure supports over 100 compliance offerings specific to the health, non-classified government, finance, education, energy, manufacturing, and media industries. Compliance offerings are obtained via formal attestations, validations, authorizations, or assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft.

Platform Protections

All platform protections described in the Appendix apply to the Regulated Industry protection case.

Customer Product stack

The following components support your regulatory requirements:

- Same as Baseline Cloud Enterprise Usage, plus
- Lockbox: the lockbox feature is deployed for every customer; however, the customer must enable this feature. The lockbox enables the customer the ability to review, approve, reject and audit access permissions granted for their customer data. A typical scenario is where a Microsoft engineer needs access to customer data in response to a support ticket.
- Encryption At Rest with Customer Managed Key: CMK for encryption at rest with CMK is separate from platform keys. The customer may provide a key to Azure Key Vault or leverage Azure Key Vault Managed HSM. By using a CMK in addition to the default Azure platform key at rest, the data achieves double encryption status.

Optional Azure Dedicated Host: provides a complete isolated compute environment through a dedicated host for the customer's isolated virtual machine.

Critical Reminders for Compute Isolation

- Azure dedicated Host and VM Isolation only applies to IaaS
- Additional information regarding compute isolation and secure IaaS solution is available online here. A video on how to benefit from dedicated host is also available online.

Profile 3: Respecting Data Geographic Boundary

Many new and emerging laws and regulations require that customers maintain their data within geographic boundaries. For this profile, Azure has several platform features which support the creation and maintenance of a data geographic boundary, including region-specific service instances with intra-region availability zones to support resiliency needs, among many others. In addition, Azure also has products you can leverage or enable to meet your requirements.

Platform Protections

All platform protections described in the Appendix apply to the data boundary case.

Customer Product stack

The following is the customer product stack that the customer must deploy/enable to realize this scenario.

- Same as Cloud Enterprise Usage for Regulated Industry plus
- Customer Managed Keys using Azure Key Vault Managed HSM: Azure Key Vault Managed HSM is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguard cryptographic keys for your cloud applications. Managed HSM does not store or process customer data outside the region the customer deploys the HSM instance in. Thus, while AKV replicates to a secondary region for disaster recovery, managed HSM does not. As an option, one can consider an alternative architecture leveraging the Azure Dedicated HSM.
- Set Azure Policy for data residency: by using the allowed locations policy in Azure Policy, and creating a custom region profile in Azure Traffic Manager, the customer can limit resource creation outside of region and limit access to in-region resources from outside of region. An easy method for deploying allowed locations policies along with a number of other residency-aligned policies is to use the Regulatory Compliance Buit-Ins available in Azure Policy. By doing so, customer data geographic protections are enabled.
- Conditional Access policy Location: should be enabled to trusted executed environment access and enforce data boundaries.

Additional information on realizing data boundary solutions, see the white paper, "Enabling Data Residency and Data Protection in Microsoft Azure Regions".

Profile 4: Reduce Unauthorized Non-Customer Data Access

Microsoft is committed to continually developing and refining a Zero-Trust model as a cloud provider. This refinement has led to ongoing product and feature development to support that model. As part of that journey, Azure actively invests in delivering solutions that span blocking access from Azure operators

to blocking Azure and customer operators. Specifically, we invest across data at rest, data in transit, and data in process in the host.

Certain customers may wish to further protect their critical data from access by their cloud provider. In these instances, customers can leverage confidential computing solutions stack to achieve their objectives, as available in the desired region(s). Stay tuned for details on Microsoft Cloud for Sovereignty as an alternative method to achieve this profile leveraging Azure Confidential Computing.

Platform Protections

All platform protections described in the Appendix apply to the reduce access case.

Customer Product stack

- Same as Cloud Enterprise Usage for Regulated Industry which includes encryption at rest and in transit along with other protections. To further reduce unauthorized non-customer access to deployed resources, particularly while data is in use, customers can choose to overlay the following series of technologies.

For those deploying VMs:

- Confidential VMs: offering that enables confidential computing virtual machines. Must be properly architected into a confidential computing solution with hardware as the root of trust as depicted in the online example. This architecture with proper configuration provides/supports the following protections:
  - Protection from physical access
  - Protection during execution
  - Protection from possession of the hardware
  - Confidential inferencing protections
  - Hardware as the root of trust
  - Select this Confidential VM for application level isolation that also provides Sensitive application logic protections and protection from all operators.

For those deploying Containers:

- Confidential Azure Kubernetes Service Nodes: confidential computing nodes can support containers and virtual machines. This architecture provides/supports the following protections.
  - Protection from physical access
  - Protection during execution
  - Protection from possession of the hardware
  - Confidential inferencing protections
  - Hardware as the root of trust
- Confidential Containers on ACI option provides all the above protections in addition to protection from all operators.

Optional Additional Confidential Services Available

- Azure Attestation Service: provides the ability to verify the identity and security posture of the platform before interacting. This service, along with internal platform processes, provides protection from a malicious service.

- Azure SQL Always Encrypted (AE): a common architectural component for confidential computing profiles. Alternatively, Azure SQL AE with enclaves should be used for confidential computing with enclave profiles.
- Azure SQL Database Ledger: a database that provides tamper protection for managing sensitive data records.
- Azure Confidential Ledger: based on permissioned blockchain model, is a highly secure confidential service that provides tamper protection for managing sensitive data records.
- Azure Key Vault Managed HSM: a managed hardware security module (HSM) service that is built using a confidential computing Trusted Execution Environment and is recommended for the highest security on customer keys stored in Azure. This architectural selection ensures the key protecting the data itself has the following protections.
    - Protection from physical access
    - Protection from possession of the hardware, and
    - Protection from all operators

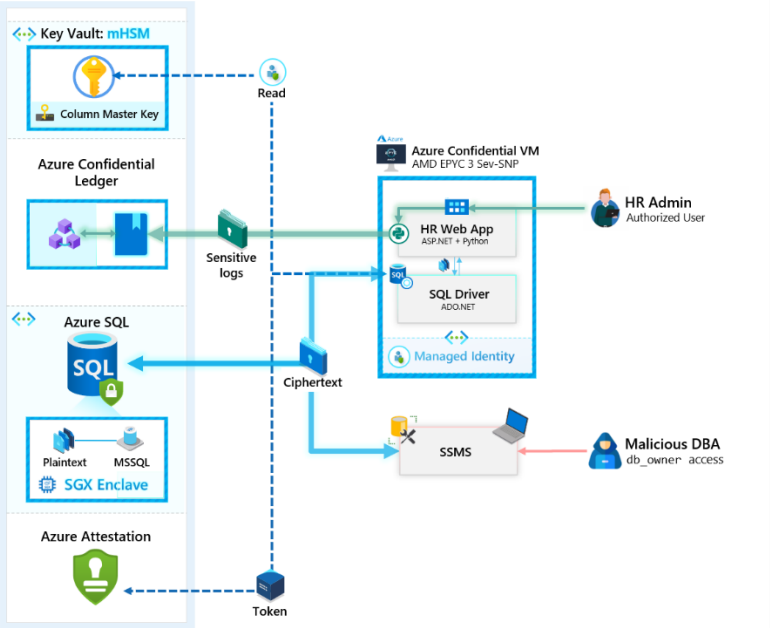
Critical reminders for Confidential Computing Solutions

- Using new technologies such as confidential computing to develop end-to-end solutions requires an understanding of the constraints created using these early services and cloud capabilities.
- SQL AE and all confidential computing feature constraints must be well-understood while architecting a confidential computing solution.

As it is early in the journey toward fully cloud-enabled confidential computing solutions, deployments will require careful planning and selection of services. Today, a fully confidential computing solution needs to consider which cloud services are required to process sensitive data and if data confidentiality needs can be met.

For additional information see our article on the web: Healthcare platform confidential computing - Azure Example Scenarios | Microsoft Docs. For a walkthrough of the example displayed in Figure 1, watch the video End-to-end Sensitive Web App with Azure Confidential Services.

Figure 1 Confidential Computing Example



Appendix of Customer Selected Data Protections

Audit of Access Permission Granted

Through the product Lockbox, customers can audit when permissions were given to the cloud provider to access their data. Note: customers must enable access to the audit logs to be able to view them as described online.

Confidential Inferencing Protections

Confidential computing solutions realized with the Intel SGX chip. The host restricts the ML hosting party from accessing both the inferencing request and corresponding response.

Customer Data Geographic Protection

Using the Allowed locations and Allowed locations for resource groups policies, the customer can enforce specific allowed locations for your data and resource deployment. By additionally using an Azure Traffic Manager custom profile with selected regions, customers can limit inbound and outbound traffic to key servers and services to only those endpoints within the regional boundary.

Encryption at Rest with Customer Managed Key

Azure allows customers to provide a key to Azure Key Vault or leverage Azure Key Vault Managed HSM that is then used along with the platform encryption keys to provide double encryption of customer data at rest.

Microsoft

Ensure Location of Data Access

For solutions that are required to ensure data boundary protections, it is possible to enable conditional access policy for a given set of locations be it countries or geographies. This conditional access policy then ensures proper location of data access.

Hardware as the Root of Trust

Azure's confidential computing platform is founded with hardware as the root of trust. Chip and hardware design is verified and supervised from the beginning, with strict supply chain controls, and audit.

Isolated Compute Environment

An isolated execution environment means a given virtual machine's execution cannot be interfered with by any other customers' executions. This is frequently leveraged for regulatory reasons, to protect against a noisy neighbor, and different licensing models. Since compute isolation comes as IaaS, customers are responsible for maintenance.

Isolate Enterprise Components

Leveraging Network Security Groups, an enterprise may isolate their own enterprise components from other aspects of the enterprise. For example, HR databases and ERP systems are frequently isolated from other enterprise data.

Managing Enterprise Access (RBAC)

One of the first steps an enterprise should do is properly establish their role-based access control over their environment exercising separation of concerns by separating those that have access to the control plane and those that control the data plane. Azure Active Directory (AAD) enables the configuration of RBAC for Azure users and groups.

Trusted Executed Environment

Also known as a TEE, this is provided by Azure's Confidential computing offerings. Confidential computing solutions, when architected correctly, provide protection during execution from the technology provider and other customers.

Trusted Inbound and Outbound Network Flows

In a cloud it is possible to add security layers to the VM networks that host the applications. Azure Virtual Network services includes firewalls and application gateways that can be used to protect inbound and outbound flows.

Protection from All Operators

Some solutions provide protection from all administrators be it tenant or customer administrators. This includes service level access.

Protection from Possession of Hardware

Data protection even in the case of possession of the hardware is provided by both Confidential Computing Enclave or Confidential Computing VM as well as Azure Key Vault managed HSM.

Protection from Malicious Service

Azure Attestation Service is a token-based service that enables an application to verify the identity and security posture of a service to demonstrate that software binaries were instantiated on a trusted platform before you interact with it. This is complemented by Microsoft's internal deployment processes including SBOM (software bill of materials) initiative in response to Executive Order (EO) 14028.

Protection While in Transit (Internet)

If a customer solution is to leverage a connection based on the internet, it is possible to lock down endpoints and achieve network isolation to only authorized callers. To achieve this protection, customers use virtual network service tags in the source of destination field as described online. Note: this customer enabled protection is complemented by the platform's encryption at rest and in transit.

Protection from Physical Access

The data within a confidential computing trusted execution environment is protected from physical access.

Reduce Risk of Data Exfiltration/Infiltration

Customer data travels across networks. By properly deploying and configuring layer 3 and layer 7 of deployed firewalls' rules, data is protected from exfiltration and infiltration.

Sensitive Application Logic Protections

The ability of confidential computing solutions to protect the logic of sensitive applications with the hardware being the root of trust.

Tamper Protection for Sensitive Records

Leveraging blockchain and immutable logs, ledger ensures records are not tampered with. May be deployed in confidential computing.

Microsoft

Appendix of Platform Protections

Accountability for Platform Changes

Azure retains immutable audit logs for all changes on the platform including all executive actions. Audit logs are stored in write once, append many, read any operations with no modify or delete operations available.

Breach Mitigation

Azure takes an assumed breach stance and continuously engages in penetration testing to identify vulnerabilities through penetration testing. This is part of the broader defense in-depth story.

Customer Identity Geographic Protection

Azure Active Directory (AAD) stores most identify information in the geographic location based on the address of the organization.

Encryption at Rest

Azure automatically protects customer's data by encrypting it at rest.

Impersonation Protection at User Level

Two-Factor authentication required for platform access.

Hardware as the Root of Trust

Azure's confidential computing platform is founded with hardware as the root of trust. Chip and hardware design is verified and supervision from the beginning, with strict supply chain controls, and audit.

Hypervisor Isolation

Hypervisor isolation is a fundamental tenant of public multi-tenant cloud computing. It is in place for every VM in Azure.

Platform Encryption at Rest and in Transit

By default, Azure encrypts all data at rest and in transit to remove vulnerabilities during these times.

Protection from Corp Identity Compromise

Part of our zero-trust model, Microsoft engineers leverage an identity separate from their corporate identities to manage the production environment adding to the depth in defense platform strategy. This approach protects the platform from corporate identity compromise as is common with phishing and malware schemes.

Protection from Known Vulnerabilities

Azure continuously scans the platform for known vulnerabilities through vulnerabilities scans.

Protection from Malware in the Platform

Azure regularly scans the platform to remove all malware detected.

Protection from Mistaken Deletes

Enabled by default, Microsoft guards against malicious or mistaken deletes with a feature referred to as Soft delete.

Protection from Malicious Platform Changes

All management is executed through secure workstation and VPN for all platform management. No persistent access is allowed.

Appendix: URLS

Allowed locations: https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#general

Regulatory Compliance Built-In Policy Initiatives (which include a significant number of the controls described above in an easily deployed structure): https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-initiatives#regulatory-compliance

Azure Active Directory: Azure Active Directory | Microsoft Azure

Azure Active Directory B2B: https://aadguide.azurewebsites.net/aadb2b/

Azure Active Directory B2C: https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview

Azure Attestation Service: Azure Attestation - Attestation Services | Microsoft Azure

Azure Compliance: Azure compliance documentation | Microsoft Docs

Azure Confidential Ledger: Microsoft Azure confidential ledger overview | Microsoft Docs

Azure Data Encryption at rest: Security Fundamentals Encryption at Rest

Azure dedicated host: https://azure.microsoft.com/en-us/services/virtual-machines/dedicated-host/

Azure Dedicated HSM: https://docs.microsoft.com/en-us/azure/dedicated-hsm/overview

Microsoft

Azure Key Vault Managed HSM: https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview#

Azure Kubernetes Service (AKS): Managed Kubernetes Service (AKS) | Microsoft Azure

Azure Secure Isolation: https://docs.microsoft.com/en-us/azure/azure-government/azure-secure-isolation-guidance

Azure Security Benchmark: Azure Security Benchmark | Microsoft Docs

Azure SQL Always Encrypted: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

Azure SQL Always Encrypted with Enclaves: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-enclaves

Azure SQL Database Ledger: Ledger overview - SQL Server | Microsoft Docs

Azure Virtual Network Services: Firewall, App Gateway for virtual networks - Azure Example Scenarios | Microsoft Docs

Compute isolation video: How to benefit from Azure Dedicated Host - YouTube

Conditional Access Policy: Conditional Access - Block access by location - Azure Active Directory | Microsoft Docs

Confidential Computing blog post: Key foundations for protecting your data with Azure confidential computing | Azure Blog and Updates | Microsoft Azure

Confidential computing build example: https://youtu.be/d2w0r-geduM

Confidential computing enclaves: https://docs.microsoft.com/en-us/azure/confidential-computing/confidential-computing-enclaves#

Confidential computing virtual machines: https://docs.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview#

Confidential computing nodes: https://docs.microsoft.com/en-us/azure/confidential-computing/confidential-nodes-aks-overview

Data infiltration/exfiltration: Traffic flow security in Azure - Azure Architecture Center | Microsoft Docs

Defense in-depth: Defense in depth security in Azure | Microsoft Docs

Github Post Confidential Computing: GitHub - mdrakiburrahman/hrapp-on-confidential-cloud: An end-to-end demonstration of a Confidential Web App running on an AMD powered Confidential VM with Azure SQL, AKV mHSM and Azure Confidential Ledger.

Customer Managed Key: Customer-managed keys for account encryption - Azure Storage | Microsoft Docs

Microsoft

Confidential computing nodes on AKS: Confidential computing nodes on Azure Kubernetes Service (AKS) | Microsoft Docs

Double Encryption: Double Encryption in Microsoft Azure | Microsoft Docs

Double Key Encryption M365: https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365-worldwide

EU Data Boundary Blog Post: https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

Healthcare Confidential Computing reference: Healthcare platform confidential computing - Azure Example Scenarios | Microsoft Docs

Hypervisors isolation: https://docs.microsoft.com/en-us/azure/security/fundamentals/hypervisor

Lockbox: https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

Microsoft Cloud for Sovereignty: Microsoft Cloud for Sovereignty: The most flexible and comprehensive solution for digital sovereignty - The Official Microsoft Blog

Microsoft Defender: https://www.microsoft.com/en-us/security/business/threat-protection

Role-Based Access Control (Azure RBAC): What is Azure role-based access control (Azure RBAC)? | Microsoft Docs

Signal: Microsoft Customer Story-Scaling secure enclave environments with Signal and Azure confidential computing

Soft Delete for containers: Soft delete for containers - Azure Storage | Microsoft Docs

Soft delete for blobs: Soft delete for blobs - Azure Storage | Microsoft Docs

SQL Always Encrypted: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15

SQL Always Encrypted with Secure Enclaves: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-enclaves?view=sql-server-ver15

Trust center: Cloud Data Integrity at its Finest | Microsoft Trust Center

Virtual network service tags: Azure service tags overview | Microsoft Docs

Whitepaper Achieving Compliant Data Residency and Security with Azure: Whitepaper Achieving Compliant Data Residency and Security with Azure - Microsoft Tech Community