Azure customer data protection

07/10/2020 • 4 minutes to read •

In this article

Access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it is only granted using a just-in-time (JIT) model using policies that are audited and vetted against our compliance and privacy policies. The access-control requirements are established by the following Azure Security Policy:

- No access to customer data, by default.
- No user or administrator accounts on customer virtual machines (VMs).
- Grant the least privilege that's required to complete task; audit and log access requests.

Azure support personnel are assigned unique corporate Active Directory accounts by Microsoft. Azure relies on Microsoft corporate Active Directory, managed by Microsoft Information Technology (MSIT), to control access to key information systems. Multi-factor authentication is required, and access is granted only from secure consoles.

All access attempts are monitored and can be displayed via a basic set of reports.

Data protection

Azure provides customers with strong data security, both by default and as customer options.

Data segregation: Azure is a multi-tenant service, which means that multiple customer deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another's data.

At-rest data protection: Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of

encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all data placed into a customer's storage account.

In-transit data protection: Microsoft provides a number of options that can be utilized by customers for securing data in transit internally within the Azure network and externally across the Internet to the end user. These include communication through Virtual Private Networks (utilizing IPsec/IKE encryption), Transport Layer Security (TLS) 1.2 or later (via Azure components such as Application Gateway or Azure Front Door), protocols directly on the Azure virtual machines (such as Windows IPsec or SMB), and more.

Additionally, "encryption by default" using MACsec (an IEEE standard at the data-link layer) is enabled for all Azure traffic travelling between Azure datacenters to ensure confidentiality and integrity of customer data.

Data redundancy: Microsoft helps ensure that data is protected if there is a cyberattack or physical damage to a datacenter. Customers may opt for:

- In-country/in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery purposes.

Data can be replicated within a selected geographic area for redundancy but cannot be transmitted outside it. Customers have multiple options for replicating data, including the number of copies and the number and location of replication datacenters.

When you create your storage account, select one of the following replication options:

- **Locally redundant storage (LRS)**: Locally redundant storage maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from a failure of a single facility.
- **Zone-redundant storage (ZRS)**: Zone-redundant storage maintains three copies of your data. ZRS is replicated three times across two to three facilities to provide higher durability than LRS. Replication occurs within a single region or across two regions. ZRS helps ensure that your data is durable within a single region.
- **Geo-redundant storage (GRS)**: Geo-redundant storage is enabled for your storage account by default when you create it. GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region. Your data is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, Azure Storage fails over to the secondary region. GRS

helps ensure that your data is durable in two separate regions.

Data destruction: When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

Customer data ownership

Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information that's entered into Azure.

Records management

Azure has established internal records-retention requirements for back-end data. Customers are responsible for identifying their own record retention requirements. For records that are stored in Azure, customers are responsible for extracting their data and retaining their content outside of Azure for a customer-specified retention period.

Azure allows customers to export data and audit reports from the product. The exports are saved locally to retain the information for a customer-defined retention time period.

Electronic discovery (e-discovery)

Azure customers are responsible for complying with e-discovery requirements in their use of Azure services. If Azure customers must preserve their customer data, they may export and save the data locally. Additionally, customers can request exports of their data from the Azure Customer Support department. In addition to allowing customers to export their data, Azure conducts extensive logging and monitoring internally.

Next steps

To learn more about what Microsoft does to secure the Azure infrastructure, see:

- Azure facilities, premises, and physical security
- Azure infrastructure availability

- Azure information system components and boundaries
- Azure network architecture

- Azure production network
- Azure SQL Database security features
- Azure production operations and management
- Azure infrastructure monitoring
- Azure infrastructure integrity

Is this page helpful?

Yes No