



# Azure Databricks Shared Responsibility Model

*For the Azure classic data  
plane*

**Databricks**  
February 2025





# Azure Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

### Azure Databricks Platform and Services

- Secure the Azure Databricks Control Plane
- Utilize industry standards and best practices to protect cloud infrastructure
- Publish CIS level 1 hardened control plane and data plane images
- Maintain a public bug bounty program
- Maintain the Azure Databricks Control Plane with updated code and images

### Azure Databricks Managed Resources

- Securely deploy and terminate Azure Databricks managed systems
- Track security configurations against industry standard baselines for systems
- Deploy the latest applicable source code and system images when new instances are launched

### Cloud Service Platform and Services

- Maintain a security management program that maintains reasonable security measures to protect customer data and services

### Identity and Access Management

- Authenticate Azure Databricks personnel using industry best practices
- Set employee privileges consistent with least privilege principles
- Limit access to systems processing customer data to employees with roles that warrant access
- Restricts access to customer content based on the principle of least privilege and segregation of duties
- Secure interactions with the customer-managed cloud account
- Secure storage and policy enforcement of secrets scope

## Customer Responsibilities

### Account and Workspace Management

- Manage account configurations, including account setup and administration, subscription management and cloud resources ([Azure](#))
- Workspace management, including workspace creation, update, and deletion, and workspace resource access ([Azure](#))

### Cluster Policies

- Configure cluster management policies and personal compute policies ([Azure](#))

### Identity and Access Management

- Enable multi-factor authentication via your Azure AD provider
- Enable System for Cross-domain Identity Management (SCIM) integration with your identity provider ([Azure](#))

### Identity, Service Principal and Access Management

- Manage users, groups, personal access tokens, and service principals ([Azure](#))
- Set Access Control Lists to restrict resource access (such as workspace objects, clusters, pools, jobs, tables) ([Azure](#))
- Secure management and use of secret scopes ([Azure](#))



Platform Security



IAM Security





# Azure Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

### Azure Databricks Managed Data

- Transmit customer content using TLS 1.2 or higher between the Customer and the Azure Databricks Control Plane and the Azure Databricks Control Plane and the Data Plane
- Encrypt customer data-at-rest within the Azure Databricks Control Plane using AES-256 bit equivalent or higher
- Delete customer content contained within a customer workspace within thirty (30) days of the workspace cancellation
- Maintain encryption hardware and services
- Encrypt data in transit and at rest, where configured
- Maintain the confidentiality, integrity and availability of data stored on CSP services

### Secure Network Communications

- Separate the Azure Databricks Control Plane from the Customer Data Plane and workspaces within the Azure Databricks Data Plane using multiple layers of network security controls
- Deploy local firewalls or security groups within the Customer Data Plane to isolate clusters
- Enable secure defaults for network access controls and security groups within the Control Plane
- Secure the physical and logical security of cloud service networking
- Maintain secure network communications for cloud services, including APIs

## Customer Responsibilities

### Data Governance

- Enable [Unity Catalog](#) within your Azure Databricks account
- Follow data governance best practices, as per your organization's requirements ([Azure](#))

### Customer-managed Data

- Secure management of data infrastructure ([Azure](#)):
  - Secure connectivity to customer-managed resources
  - Secure service integration with Azure Databricks ([Azure](#))
  - Enable Data Plane [local disk encryption](#) or [inter-cluster encryption](#)

### Customer-managed Encryption Keys

- Deploy customer-managed encryption keys (CMK) ([Azure](#))
  - Enable CMK for managed services
  - Enable CMK for workspace storage

### Cloud Network Security

- Configure Secure Cluster Connectivity ([Azure](#))
- Enable customer-managed networks ([Azure VNet](#))
- Configure Data Exfiltration Protection according to your organization's data protection policy ([Azure](#))

### IP Access Control Lists and Private Link

- Configure Azure Databricks workspace IP access lists ([Azure](#))
- Configure Private Link access for Users → Control Plane and Control Plane → Data Plane connections ([Azure](#))



Data  
Security



Network  
Security





# Azure Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

### Security Monitoring

- Deploy security detection capabilities, including those provided natively by Cloud Service Providers
- Generate audit logs from customer's use of the platform services and retain them for at least one year
- Deliver audit logs from the customer's use of the platform services based on the customer's configuration (Premium subscriptions and above)
- Deploy a dedicated Detection engineering team that develops intrusion detection monitoring across its computing resources
- Employ an incident response framework to manage and minimize the effects of unplanned security events
- Notify customers of security breaches in accordance with data protection laws and customer agreements

### Secure Code Execution

- Maintain secure cloud infrastructure
- Maintain availability and security of the job scheduler
- Secure delivery of customer code (such as notebooks, repos and models, queries) from the control plane to the data plane

### Vulnerability and Patch Management

- Maintain a vulnerability management program that follows industry best practices, performs daily and weekly authenticated vulnerability scans against Databricks infrastructure and services
- Regularly release updated data plane images with patches that meet Security Addendum patch SLAs

## Customer Responsibilities

### Audit Log Configuration

- Enable Azure Databricks System Tables for system and performance monitoring ([Azure](#))
- Alternatively, configure Azure Databricks diagnostic log delivery to your cloud storage ([Azure](#))
- Configure verbose audit logs for your workspace(s) ([Azure](#))

### Account and Workspace Security Monitoring

- Deploy account and workspace [security monitoring](#)
- Deploy cloud service security monitoring
- Investigate and respond to potential security incidents related to customer-managed features, services and resources

### Application Security

- Perform security reviews of your code, libraries and jobs, such as notebooks ([Azure](#)), [Terraform](#), and third-party libraries ([Azure](#))

### CI/CD Pipeline and Repo Integration

- Integrate Git with Azure Databricks repos ([Azure](#))
- Manage CI/CD Pipeline integration with Azure Databricks ([Azure](#))

### Vulnerability and Patch Management

- Restart active clusters to deploy instances with the latest patches ([Azure](#))
- Optionally, configure Automatic cluster update to automate cluster restarts during maintenance windows ([Azure](#))



## Security Monitoring



## Code Execution / Jobs



## Vulnerability & Patch Management





# Azure Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

## Customer Responsibilities



### Core Compliance

#### Standards and Compliance

- Maintain independent third-party audits, standards, and certifications that apply to all customer environments:
  - ISO 27001, 27017, 27018
  - SOC 2 Type II, SOC 1 Type II, SOC 3
- Provide tools and configurations that enable use of services in compliance with applicable laws (such as GDPR and CCPA)

*\* Additional compliance standards covered later, such as HIPAA, FedRAMP, PCI*

#### Maintain Adherence to Relevant Compliance and Standards:

- When using Azure Databricks to process sensitive data such as PII, adhere to relevant privacy regulations such as the GDPR and CCPA
- Review your compliance needs and add optional compliance service offering where required (such as for FedRAMP, PCI-DSS, HIPAA)
- Comply with applicable laws when using Azure Databricks, including by implementing any required configurations in accordance with Azure Databricks documentation



### Disaster Recovery

#### Maintain Disaster Recovery Capabilities\* For:

- Review Business Continuity and Disaster Recovery plans annually
- Conduct Business Continuity and Disaster Recovery drills annually
- Conduct periodic backups of the Azure Databricks Control Plane\*
- Maintain the cloud service availability and capacity

#### Data Backups

- Backup of your organization's [account and workspace](#)
- Set [Recovery Point Objectives](#) (RPO) and [Recovery Time Objectives](#) (RTO) using best practices ([Azure](#))

#### Multi-region Workspace Deployment

- Perform a [Disaster Recovery Impact Assessment](#)
- Deploy Disaster Recovery services for Azure Databricks to meet the organization's DR requirements ([Azure](#))



### Security Best Practices

#### Employ Security Best Practices

- Periodically review cryptographic standards to select and update technologies and ciphers in accordance with assessed risk and market acceptance of new standards
- Conduct third-party penetration tests at least annually
- Employ an in-house offensive security team

#### Multi-region Workspace Deployment

- Adopt Azure Databricks security best practices based on the organization's cybersecurity requirements ([Azure](#))
- Follow security best practices for the customer's cloud environment ([Azure](#))



# Azure Serverless Shared Responsibility Model





# Azure Databricks Managed Serverless Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

### Databricks Platform and Services

- Secure the Databricks Control Plane
- Utilize industry standards to harden images and operating systems deployed under our control
- Maintain a public bug bounty program
- Maintain the Databricks Control Plane with updated code and images

### Databricks Managed Resources

- Securely deploy and terminate Databricks managed systems
- Track security configurations against industry standard baselines for systems under Databricks control
- Deploy the latest code and system images upon launch of customer Compute Plane hosts

### Cloud Service Platform and Services

- Maintain security of the cloud service infrastructure

### Identity and Access Management

- Authenticate Databricks personnel using industry best practices
- Set employee privileges consistent with least privilege principles
- Limit access to systems processing customer data to employees with roles that warrant access
- Restrict access to customer content based on the principle of least privilege and segregation of duties
- Secure storage and policy enforcement of secrets scope
- Maintain access controls required to restrict access to authorized customer resources
- Restrict employee access to customer resources`

## Customer Responsibilities

### Account and Workspace Management

- Manage account configurations, including account setup and administration, subscription management and cloud resources ([Azure](#))
- Workspace management, including workspace creation and update, and workspace resource access ([Azure](#))

### Identity and Access Management

- Enable multifactor authentication via your SSO provider
- Enable SCIM integration with your identity provider ([Azure](#))

### Identity, Service Principal and Access Management

- Manage users, groups, personal access tokens, and service principals ([Azure](#))
- Set Access Control Lists to restrict access (such as workspace objects, serverless endpoints, jobs, tables) ([Azure](#))
- Secure management and use of secret scopes ([Azure](#))



Platform Security



IAM Security







# Azure Databricks Managed Serverless Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

### Databricks Managed Data

- Encrypt Databricks communications between the Databricks Control Plane and the customer workspace using TLS 1.2 or higher
- Encrypt customer data-at-rest within the Databricks Control Plane using AES-256 bit equivalent or higher
- Delete customer content contained within a customer workspace within thirty (30) days of the workspace cancellation
- Enable local disk encryption for serverless drives
- Maintain encryption hardware and services
- Maintain the confidentiality, integrity and availability of data stored on CSP services

### Cloud Network Security

- Configure Private Link from Control Plane to the Serverless Compute Plane

### Secure Network Communications

- Separate the Databricks Control Plane from the Databricks Compute Plane and workspaces within the Databricks Compute Plane using multiple layers of network security controls
- Deploy local firewalls or security groups within the Databricks Compute Plane to isolate clusters
- Enable secure defaults for network access controls and security groups within the Control Plane
- Secure the physical and logical security of cloud service networking
- Maintain secure network communications for cloud services, including APIs

## Customer Responsibilities

### Data Governance

- Enable [Unity Catalog](#) within your Databricks account
- Follow data governance best practices, as per your organization's requirements ([Azure](#))

### Customer-Managed Data

- Secure management of data infrastructure ([Azure](#)):
  - Secure service integration with Databricks ([Azure](#))
  - Configure the Azure Storage Firewall ([Azure](#))

### Customer-Managed Encryption Keys

- Enable customer-managed encryption keys (CMK), where required ([Azure](#))
  - Enable CMK for managed services
  - Enable CMK for workspace storage

### IP Access Control Lists and Private Link

- Configure Databricks workspace IP access lists ([Azure](#))
- Configure Private Link for user access to the Control Plane ([Azure](#))



Data  
Security



Network  
Security







# Azure Databricks Managed Serverless Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

## Customer Responsibilities

### Security Monitoring

- Monitor for security violations of the underlying cloud service infrastructure and services
- Generate audit logs from customer's use of the platform services and retain them for at least one year (Premium subscription required)
- Deliver audit logs from the customer's use of the platform services based on customer configurations (Premium subscription required)
- Deploy a dedicated Detection engineering team that develops intrusion detection monitoring across its computing resources
- Employ an incident response framework to manage and minimize the effects of unplanned security events
- Notify customers of security breaches in accordance with data protection laws and customer agreements
- Deploy security monitoring for tenant isolation in the serverless compute plane

### Audit Log Configuration

- Enable Azure Databricks System Tables for system and performance monitoring ([Azure](#))
- Alternatively, configure Azure Databricks diagnostic log delivery to your cloud storage ([Azure](#))
- Configure verbose audit logs for your workspace(s) ([Azure](#))

### Account and Workspace Security Monitoring

- Deploy account and workspace security monitoring
- Investigate and respond to potential security incidents in your Databricks account and workspace(s) for systems under your control

### Secure Code Execution

- Maintain secure cloud infrastructure
- Maintain availability and security of the job scheduler
- Secure delivery of customer code (such as notebooks, repos and models, queries) from the control plane to the compute plane

### Application Security

- Perform security reviews of your code, libraries and jobs, such as notebooks ([Azure](#)), [Terraform](#), and third-party libraries ([Azure](#))

### CI/CD Pipeline and Repo Integration

- Integrate Git with Databricks repos ([Azure](#))
- Manage CI/CD Pipeline integration with Databricks ([Azure](#))

### Vulnerability and Patch Management

- Maintain a vulnerability management program that follows industry best practices, performs daily and weekly authenticated vulnerability scans against cloud serverless infrastructure and services
- Regularly release updated data plane images with patches that meet patch management SLAs
- Restart active serverless clusters after seven days to deploy instances with the latest patches

### Vulnerability and Patch Management

- Restart active serverless clusters to deploy instances with the latest patches (if required before the cluster is active for seven days) ([Azure](#))



Security Monitoring



Code Execution / Jobs



Vulnerability & Patch Management



# Azure Databricks Managed Serverless Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

## Customer Responsibilities



### Core Compliance

#### Standards and Compliance

- Maintain independent third-party audits, standards, and certifications that apply to all customer environments:
  - ISO 27001, 27017, 27018
  - SOC 2 Type II, SOC 1 Type II, SOC 3
- Enable compliant workflows supported by [Databricks](#)

#### Maintain adherence to relevant compliance and standards:

- Comply with applicable laws and regulations
- When using Databricks to process sensitive data such as PII, adhere to relevant privacy regulations such as the GDPR and CCPA



### Disaster Recovery

#### Maintain Disaster Recovery\* capabilities for:

- Review Business Continuity and Disaster Recovery plans annually
- Conduct Business Continuity and Disaster Recovery drills annually
- Conduct periodic backups of the Databricks Control Plane\*

#### Data Backups

- Backup of your organization's [account and workspace](#)
- Set [Recovery Point Objectives](#) (RPO) and [Recovery Time Objectives](#) (RTO) using best practices ([Azure](#))

#### Multi-region Workspace Deployment

- Perform a [Disaster Recovery Impact Assessment](#)
- Deploy Disaster Recovery services for Databricks to meet the organization's DR requirements ([Azure](#))



### Security Best Practices

#### Employ security best practices

- Periodically review cryptographic standards to select and update technologies and ciphers in accordance with assessed risk and market acceptance of new standards
- Regularly run authenticated vulnerability scans against representative hosts in the SDLC pipeline
- Conduct third-party penetration tests at least annually
- Employ an in-house offensive security team

#### Multi-region Workspace Deployment

- Adopt Databricks security best practices based on the organization's cyber risk appetite ([Azure](#))
- Follow security best practices for the customer's cloud environment ([Azure](#))





# Databricks ESM/CSP Shared Responsibility Model





# Azure Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Azure Databricks and the Azure Databricks customer. For their part, Azure has formalized their [shared responsibility model](#).

## Azure Databricks Responsibilities

## Customer Responsibilities



### Enhanced Security Monitoring

#### Databricks Enhanced Security Monitoring (ESM) Responsibilities

- Deploy ESM instances with enhanced CIS Level 1 hardening
- Deploy antivirus, behavior-based malware and file integrity monitoring
- Provide vulnerability reports of the host OS upon request
- Enable FIPS 140-2 Level 1 mode encryption on ESM instances
- Maintain security of the cloud service infrastructure

#### Customer Enhanced Security Monitoring Responsibilities

- Enable Enhanced Security Monitoring on relevant workspace(s)
- Monitor enhanced event logs for security incidents
- Restart ESM clusters to deploy the latest patched instances and agent signatures
- Provide the destination Email for vulnerability reports delivery



### Compliance Security Profile

#### Databricks Compliance Security Profile (CSP) Responsibilities

- Enable ESM security enhancements (listed above)
- Restart clusters that run past the maintenance window to deploy the latest patches
- Enumerate preview features that are usable within HIPAA, PCI
- Maintain security of the cloud service infrastructure

#### Customer Compliance Security Responsibilities

- Prepare workspace(s) for the compliance security profile
- Enable the Compliance Security Profile on relevant workspace(s)



### HIPAA, PCI

#### Databricks HIPAA and PCI Responsibilities

- Complete annual HIPAA, PCI-DSS audits (region and cloud specific)
- Provide HIPAA and PCI compliant internal services
- Enforce Enterprise Security Monitoring and Compliance Security Profile features

#### Customer HIPAA and PCI Responsibilities

- Enable Compliance Security Profile on relevant workspaces
- Use only supported preview features (PCI)
- Comply with compliance-specific requirements (Azure)
- Comply with the PCI Shared Responsibility Model requirements



### GDPR/CCPA

#### Databricks GDPR/CCPA Service Responsibilities

- Provide service that are GDPR/CCPA compliant (subject to customer responsibilities)

#### Customer GDPR/CCPA Service Responsibilities

- Maintain GDPR/CCPA compliant usage of Databricks services

