databricks

Databricks Shared Responsibility Model

For the AWS classic data plane

Databricks
July 2023

Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Platform Security	**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 applicable source code and system images upon launch of customer Data Plane hosts	**Account and Workspace Management** • Manage account configurations, including account setup and administration, subscription management and cloud resources (AWS) • Workspace management, including workspace creation, update, and deletion, and workspace resource access (AWS) **Cluster Policies** • Configure cluster management policies and personal compute policies (AWS) **Instance Management** • Restart workspace cluster VMs as needed to deploy the latest patched images and code in accordance with patch management policy (AWS)	**Cloud Service Platform and Services** • Maintain security of the cloud service infrastructure • Maintain a security management program that maintains reasonable security measures to protect customer data and services
IAM Security	**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 • 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	**Identity and Access Management** • Setup Single Sign-on and password access controls for Databricks account and workspace(s) (AWS) • Enable multi-factor authentication via your SSO provider • Enable System for Cross-domain Identity Management (SCIM) integration with your identity provider (AWS) **Identity, Service Principal and Access Management** • Manage users, groups, personal access tokens, and service principals (AWS) • Set Access Control Lists to restrict resource access (such as workspace objects, clusters, pools, jobs, tables) (AWS) • Use least-privilege principles for cross-account IAM roles (AWS) • Secure management and use of secret scopes (AWS)	**Identity and Access Management** • Maintain access controls required to restrict access to authorized customer resources • Restrict employee access to customer resources

Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Data Security	**Databricks Managed Data** • Transmit customer content using TLS 1.2 or higher between the Customer and the Databricks Control Plane and the Databricks Control Plane and the Data Plane • 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	**Data Governance** • Enable Unity Catalog within your Databricks account • Follow data governance best practices, as per your organization's requirements (AWS) **Customer-managed Data** • Secure management of data infrastructure (AWS): ○ Secure connectivity to customer-managed resources ○ Secure service integration with Databricks (AWS) **Customer-managed Encryption Keys** • Deploy customer-managed encryption keys (CMK) (AWS) ○ Enable CMK for managed services ○ Enable CMK for workspace storage	**Cloud Service Managed Data** • 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 • Enable Spark inter-cluster encryption (AWS Nitro that support in-transit encryption) • Enable Data Plane local disk encryption (AWS Nitro or NVMe)
Network Security	**Secure Network Communications** • Separate the Databricks Control Plane from the Customer Data Plane and workspaces within the 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	**Cloud Network Security** • Configure Secure Cluster Connectivity (AWS) • Enable customer-managed networks (AWS VPC) • Configure Data Exfiltration Protection according to your organization's data protection policy (AWS) **IP Access Control Lists and Private Link** • Configure Databricks workspace IP access lists (AWS) • Configure Private Link access for Users → Control Plane and Control Plane → Data Plane connections (AWS)	**Secure Network Communications** • Secure the physical and logical security of cloud service networking • Maintain secure network communications for cloud services, including APIs

Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Security Monitoring	**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 (Premium subscription+) • Deliver audit logs from the customer's use of the platform services based on the customer's configuration (Premium subscriptions+) • 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	**Audit Log Configuration** • Configure Databricks audit log delivery to your cloud storage (AWS) • Configure verbose audit logs for your workspace(s) (AWS) **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	**Security Monitoring** • Monitor for security violations of the underlying cloud service infrastructure and services • Deliver audit logs for cloud service events based on customer configurations • Employ an incident response framework • Notify customer of a security breach for which that customer is impacted
Code Execution / Jobs	**Secure Code Execution** • 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	**Application Security** • Perform security reviews of your code, libraries and jobs, such as notebooks (AWS), Terraform, and third-party libraries (AWS) **CI/CD Pipeline and Repo Integration** • Integrate Git with Databricks repos (AWS) • Manage CI/CD Pipeline integration with Databricks (AWS)	**Secure Code Execution** • Maintain secure cloud infrastructure

Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud 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
	
	** Additional compliance standards covered later, such as HIPAA, FedRAMP, PCI*
		Maintain Adherence to Relevant Compliance and Standards:
		• When using 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 and regulations
			Standards and Compliance
			• Maintain independent third party audit, standards and certifications
			• Maintain compliant services

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 (AWS) **Multi-region Workspace Deployment** • Perform a Disaster Recovery Impact Assessment • Deploy Disaster Recovery services for Databricks to meet the organization's DR requirements (AWS)	**Disaster Recovery capabilities** • Cloud service capacity • Review Business Continuity and Disaster Recovery plans annually • Conduct Business Continuity and Disaster Recovery drills annually
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 • Maintain a vulnerability management program that follows industry best practices • 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 cybersecurity requirements (AWS) • Follow security best practices for the customer's cloud environment (AWS)	**Employ Security Best Practices** • Review cryptographic standards • Regularly run authenticated vulnerability scans • Address vulnerabilities within SLAs • Conduct third-party penetration tests

**Note: Databricks doesn't provide backup or disaster recovery services. Disaster Recovery plans and control plane backups are for resiliency purposes in the case of a critical systems failure and Databricks is not able to restore specific data based on a customer request*

AWS Serverless Shared Responsibility Model

Databricks Managed Serverless Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Platform Security	**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 applicable source code and system images upon launch of customer Compute Plane hosts	**Account and Workspace Management** • Manage account configurations, including account setup and administration, subscription management and cloud resources (AWS) • Workspace management, including workspace creation, update, and deletion, and workspace resource access (AWS)	**Cloud Service Platform and Services** • Maintain security of the cloud service infrastructure • Maintain a security management program that maintains reasonable security measures to protect customer data and services
IAM Security	**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 interactions with the customer-managed cloud account • Secure storage and policy enforcement of secrets scope	**Identity and Access Management** • Setup Single Sign-on and password access controls for Databricks account and workspace(s) (AWS) • Enable multifactor authentication via your SSO provider • Enable SCIM integration with your identity provider (AWS) **Identity, Service Principal and Access Management** • Manage users, groups, personal access tokens, and service principals (AWS) • Set Access Control Lists to restrict access (such as workspace objects, serverless endpoints, jobs, tables) (AWS) • Use least-privilege principles for cross-account IAM roles (AWS) • Secure management and use of secret scopes (AWS)	**Identity and Access Management** • Maintain access controls required to restrict access to authorized customer resources • Restrict employee access to customer resources

Databricks Managed Serverless Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Data Security	**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	**Data Governance** • Enable Unity Catalog within your Databricks account • Follow data governance best practices, as per your organization's requirements (AWS) **Customer-Managed Data** • Secure management of data infrastructure (AWS): ◦ Secure connectivity to customer-managed resources **Customer-Managed Encryption Keys** • Enable customer-managed encryption keys (CMK), where required (AWS) ◦ Enable CMK for managed services ◦ Enable CMK for workspace storage	**Cloud Service Managed Data** • 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 • Enable Compute Plane local disk encryption (AWS Nitro or NVMe)
Network Security	**Cloud Network Security** • Configure secure connectivity from the 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	**IP Access Control Lists and Private Link** • Configure Databricks workspace IP access lists (AWS) • Configure Private Link for user access to the Control Plane (AWS) • Configure Data Exfiltration Protection according to your organization's data protection policy (AWS)	**Secure Network Communications** • Secure the physical and logical security of cloud service networking • Maintain secure network communications for cloud services, including APIs

Databricks Managed Serverless Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Security Monitoring	**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 (Premium subscription+) • Deliver audit logs from the customer's use of the platform services based on customer configurations (Premium subscription+) • 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** • Configure Databricks audit log delivery to your cloud storage (AWS) • Configure verbose audit logs for your workspace(s) (AWS) **Account and Workspace Security Monitoring** • Deploy account, workspace security monitoring • Investigate and respond to potential security incidents in your Databricks account and workspace(s) for systems under your control	**Security Monitoring** • Monitor for security violations of the underlying cloud service infrastructure and services • Deliver audit logs for cloud service events based on customer configurations • Employ an incident response framework • Notify customer of a security breach for which that customer is impacted
Code Execution / Jobs	**Secure Code Execution** • 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 (AWS), Terraform, and third-party libraries (AWS) **CI/CD Pipeline and Repo Integration** • Integrate Git with Databricks repos (AWS) • Manage CI/CD Pipeline integration with Databricks (AWS)	**Secure Code Execution** • Maintain secure cloud infrastructure

Databricks Managed Serverless Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud 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
			Standards and Compliance
			• Maintain independent third party audit, standards and certifications
			• Enable compliant workflows supported by the cloud vendor

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 (AWS) **Multi-region Workspace Deployment** • Perform a Disaster Recovery Impact Assessment • Deploy Disaster Recovery services for Databricks to meet the organization's DR requirements (AWS)	**Disaster Recovery capabilities** • Cloud service capacity • Review Business Continuity and Disaster Recovery plans annually • Conduct Business Continuity and Disaster Recovery drills annually
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 (AWS) • Follow security best practices for the customer's cloud environment (AWS)	**Employ security best practices** • Review cryptographic standards • Regularly run authenticated vulnerability scans • Address vulnerabilities within SLAs • Conduct third-party penetration tests

*Note: Databricks doesn't provide backup or disaster recovery services. Disaster Recovery plans and control plane backups are for resiliency purposes in the case of a critical systems failure and Databricks is not able to restore specific data based on a customer request

Databricks ESM/CSP
Shared Responsibility Model

Databricks Managed Services Shared Responsibility Model

Security and compliance are a shared responsibility between Databricks, the Databricks customer, and the cloud service provider (CSP) AWS. For their part, AWS has formalized their shared responsibility model.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud 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 • Leverage FIPS 140-2 Level 1 encryption services where available	**Customer Enhanced Security Monitoring Responsibilities** • Enable Enhanced Security Monitoring on relevant workspace(s) • Monitor enhanced event logs for for security incidents • Restart ESM clusters to deploy the latest patched instance versions and agent signatures before the maintenance window [if required] • Provide the destination Email for vulnerability reports delivery	**CSP ESM Responsibilities** • Maintain security of the cloud service infrastructure
Compliance Security Profile	**Databricks Compliance Security Profile (CSP) Responsibilities** • Enable ESM security enhancements (listed above) • Enforcement of AWS Nitro instances on CSP workspace(s) • Restart clusters running past the maintenance window to deploy the latest patches	**Customer Compliance Security Responsibilities** • Prepare workspace(s) for the compliance security profile • Enable the Compliance Security Profile on relevant workspace(s) (AWS)	**CSP Compliance Responsibilities** • Maintain security of the cloud service infrastructure

HIPAA, PCI, DoD and FedRAMP	**Databricks HIPAA, PCI and FedRAMP Responsibilities**
	• Complete annual HIPAA, PCI-DSS, FedRAMP audits (region and cloud specific)
	• Provide HIPAA, PCI and FedRAMP (Moderate on AWS) compliant internal services
	• Enforce Enterprise Security Monitoring and Compliance Security Profile features
		Customer HIPAA, PCI, FedRAMP Responsibilities
		• Enable Compliance Security Profile on relevant workspaces (AWS)
		• Use only supported preview features (PCI, HIPAA)
		• Comply with compliance-specific prerequisites:
		  ○ Detailed docs: AWS: HIPAA, PCI, FedRAMP
		  ○ Obtain entitlement to process regulated data on Databricks
		  ○ Comply with the PCI Shared Responsibility Model (PCI)
		  ○ Follow FedRAMP PMO documentation requirements (FedRAMP)
			CSP HIPAA, PCI and FedRAMP Responsibilities
			• Complete annual HIPAA, PCI-DSS, FedRAMP audits

GDPR/CCPA	**Databricks GDPR/CCPA Service Responsibilities** • Provide services that are GDPR/CCPA compliant (subject to customer responsibilities)	**Customer GDPR/CCPA Service Responsibilities** • Maintain GDPR/CCPA compliant usage of Databricks services	**CSP GDPR/CCPA Responsibilities** • Provide service that are GDPR/CCPA compliant