databricks

Databricks Shared Responsibility Model

For the GCP classic data plane

Databricks
February 2025

Databricks Managed Services Shared Responsibility Model

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

	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 (GCP) • Workspace management, including workspace creation, update, and deletion, and workspace resource access (GCP) **Cluster Policies** • Configure cluster management policies and personal compute policies (GCP)	**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** • Enable multi-factor authentication via your SSO provider • Enable System for Cross-domain Identity Management (SCIM) integration with your identity provider (GCP) **Identity, Service Principal and Access Management** • Manage users, groups, personal access tokens, and service principals (GCP) • Set Access Control Lists to restrict resource access (such as workspace objects, clusters, pools, jobs, tables) (GCP) • Secure management and use of secret scopes (GCP)	**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) GCP. For their part, GCP has a formalized their shared responsibility models.

	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 (GCP)
		Customer-managed Data
		• Secure management of data infrastructure (GCP):
		  ○ Secure connectivity to customer-managed resources
		  ○ Secure service integration with Databricks (GCP)
			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 (GCP)
			• Enable Data Plane local disk encryption (GCP)

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 (GCP) • Enable customer-managed networks (GCP VPC) • Configure Data Exfiltration Protection according to your organization's data protection policy (GCP) **IP Access Control Lists and Private Link** • Configure Databricks workspace IP access lists (GCP)	**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) GCP. For their part, GCP has a formalized their shared responsibility models.

	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 • 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	**Audit Log Configuration** • Configure Databricks audit log delivery to your cloud storage (GCP) • Configure verbose audit logs for your workspace(s) (GCP) **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 (GCP), Terraform, and third-party libraries (GCP) **CI/CD Pipeline and Repo Integration** • Integrate Git with Databricks repos (GCP) • Manage CI/CD Pipeline integration with Databricks (GCP)	**Secure Code Execution** • Maintain secure cloud infrastructure
Vulnerability & Patch Management	**Patching and Vulnerability 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 our Security Addendum patch SLAs	**Patching and Vulnerability Management** • Restart workspace cluster VMs as needed to deploy the latest patched images and code in accordance with patch management policy (GCP)	**Scan and Patch Cloud Infrastructure** • Scan and patch the cloud's infrastructure, firmware and software, etc. it manages, such as networking, servers, and virtualization

Databricks Managed Services Shared Responsibility Model

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

	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
	• 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 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 Databricks, including by implementing any required configurations in accordance with Databricks documentation
			Standards and Compliance
			• Maintain independent third party audit, standards and certifications
			• Maintain relevant independent third-party audits, standards, and certifications
			• Maintain relevant 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 (GCP) **Multi-region Workspace Deployment** • Perform a Disaster Recovery Impact Assessment • Deploy Disaster Recovery services for Databricks to meet the organization's DR requirements (GCP)	**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 • 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 (GCP) • Follow security best practices for the customer's cloud environment (GCP)	**Employ Security Best Practices** • Follow industry best practices • Review cryptographic standards • 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*

GCP Serverless 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) GCP. For their part, GCP has a formalized their shared responsibility models.

	Databricks Responsibilities	*Customer Responsibilities*	*Cloud Responsibilities*
Platform Security	**Databricks Platform and Services** • Secure the Databricks Control Plane • Utilize industry standards to protect Databricks infrastructure • Deploy CIS level 1 hardened control plane and data plane images • 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 (GCP) • Workspace management, including workspace creation, update, and deletion, and workspace resource access (GCP)	**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** • Enable multifactor authentication via your SSO provider • Enable SCIM integration with your identity provider (GCP) **Identity, Service Principal and Access Management** • Manage users, groups, personal access tokens, and service principals (GCP) • Set Access Control Lists to restrict access (such as workspace objects, serverless endpoints, jobs, tables) (GCP) • Secure management and use of secret scopes (GCP)	**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) GCP. For their part, GCP has a formalized their shared responsibility models.

	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 (GCP) **Customer-Managed Data** • Secure management of data infrastructure (GCP): ◦ Secure connectivity to customer-managed resources **Customer-Managed Encryption Keys** • Enable customer-managed encryption keys (CMK), where required (GCP): ◦ 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
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 (GCP) • Configure Private Service Connect for user access to the Control Plane (GCP) • Configure Data Exfiltration Protection according to your organization's data protection policy (GCP)	**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) GCP. For their part, GCP has a formalized their shared responsibility models.

	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+) • 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 (GCP) • Configure verbose audit logs for your workspace(s) (GCP) **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 (GCP), Terraform, and third-party libraries (GCP) **CI/CD Pipeline and Repo Integration** • Integrate Git with Databricks repos (GCP) • Manage CI/CD Pipeline integration with Databricks (GCP)	**Secure Code Execution** • Maintain secure cloud infrastructure
Vulnerability & Patch Management	**Patching and Vulnerability Management** • Maintain a vulnerability management program that follows industry best practices, performs daily and weekly authenticated vulnerability scans against Databricks serverless infrastructure and services • Regularly release updated serverless images with patches that meet our Security Addendum patch SLAs • Restart active clusters after seven (7) days	**Restart Clusters to Deploy the Latest Patches** • Restart active serverless clusters to deploy instances with the latest patches (if required before the cluster is active for seven days) (GCP)	**Scan** • Scan and patch the cloud's infrastructure, firmware and software, etc. it manages, such as networking, servers, and virtualization

Databricks Managed Services Shared Responsibility Model

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

	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 (GCP) **Multi-region Workspace Deployment** • Perform a Disaster Recovery Impact Assessment • Deploy Disaster Recovery services for Databricks to meet the organization's DR requirements (GCP)	**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 • 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 (GCP) • Follow security best practices for the customer's cloud environment based on the organization's cyber risk appetite (GCP)	**Employ security best practices** • Follow industry best practices • Review cryptographic standards • 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