Descartes Labs

Find. Monitor. Predict.

Descartes Labs Platform Privacy & Security

What We Do Today

Descartes Labs is dedicated to providing the highest level of security to our customers and partners. For this reason, we have compiled a set of security safeguards and procedures, outlined below.

Data

- Descartes Labs provides AES-256 encryption for both data-at-rest and data-in-transit; and our platform is configured to rotate encryption keys automatically.
- Each user's data is isolated in its own object-store.
- All customer data is in an isolated project. This project has no servers, API's, or public-facing IP's. Users of Descartes Labs API's do not have direct access to native object storage. All user access is routed through Descartes Labs API and its IAM role permissions where access is audited and logged.
- Development and Staging infrastructure do not have direct access to customer data.
- End-user accounts do not have direct access to user data or the isolated Cloud project with data. Access is granted through the API and the API's authentication and authorization.
- All customer data is stored in the US and has redundant failover replicas provided automatically by our cloud vendor.
- User access verified by 3rd party, that user A can not access user B's data.
- Our platform uses TLS for Internet-facing web services (e.g. APIs and web front-ends).
- Descartes Labs does not store customer information on external services outside our platform hosting provider. We do not, under any circumstances, put customer information on removable media such as thumb drives, DVDs, CDs, Zip-drives, 8-tracks, etc. We may receive data in some instances for large geospatial files if that is the preferred method of distribution, but we must handle this under customer oversight.
- Our platform utilizes our cloud service provider's secure deletion process to remove customer data from our systems. Backed up data is securely deleted according to that data's retention period.
- Domain certificates are stored in encrypted form at rest and are accessible by a limited set of platform administrators.
- Descartes Labs employee computers utilize BitLocker to provide encryption at rest.

Compute

- Descartes Labs Tasks allow scaled out analytics against PB's of data.
- Each user's compute via the DL-Tasks API, is a network isolated workspace, which scales independently of other users.
- All end-user access to the host cluster control place is blocked only allowing access to Descartes Labs API's

Security Monitoring

- All Descartes Labs API's are behind the Global Load balancers provided by our cloud vendor. These have white/blacklist capabilities, as well as DDOS/XSS/SQL injection mitigation.
- All resources are by default blocked on our cloud vendor's firewall. To open traffic internally or to the public requires an explicitly opening of a firewall port. All firewalls are checked in and versioned as code, requiring a peer-reviewed pull request to be modified
- The Descartes Labs platform undergoes frequent vulnerability scanning, leverages IDS/IPS capabilities from our platform hosting provider via Cloud Armor and Security Command Center to detect, alert, and block suspicious and malicious behavior. The feeds include information from both network events, internal-system events, and vulnerability / threat intelligence feeds.
- Our platform resources are configured with verbose logging enabled and postured to detect unauthorized communications that subsequently trigger our response process which is automated to the greatest extent possible to enable rapid response actions to identify indicators of compromise/attack (IOCs/IOAs).

Availability:

Descartes Labs publishes availability and outages of all general availability services on:

https://status.descarteslabs.com/

1704 B Llano #403, Santa Fe NM, 87505 | www.descarteslabs.com

Descartes Labs

Find. Monitor. Predict.

Descartes Labs Platform Privacy & Security

Change Control

- All infrastructure is written as code.
- All IaC code is versioned and checked into source control.
- All changes require an SRE/Security PR peer review
- All changes are automatically applied with service accounts.
- All code is built through a centralized build and test system and has automatic security scans on the build artifacts against a known vulnerability database.

Third-party Security Assessment

- Descartes Labs has an independent 3rd party evaluation its security externally every quarter.
- Descartes Labs maintains our ISO 27001:2013 certification.
- Descartes Labs leverages various third-party service providers to conduct (at minimum) an annual external and internal penetration test of our platform and corporate environment to proactively remediate identified vulnerabilities, misconfigurations, or other risks.

Authentication & Authorization

- Descartes Labs Platform Identity management system is Auth0.
- Descartes Labs currently allows two social providers identities (Google and Github) or allows the creation of an account, persisted in Auth0.
- All passwords stored in Auth0 are encrypted and not visible to Descartes Labs.
- All IAM platform and policies are in Auth0.
- Only a limited number of Descartes Labs employees have been approved for Auth0 admin access.
- All Auth0 authentication and changes are logged.

Public Talks:

Descartes Labs describes infrastructure and security

Kubernetes multi-tenancy security with gVisor GKE Sandbox »
Kubernetes & Istio service mesh for multi-tenancy application »

Administration

- Descartes Labs corporate identity system is Google Gsuite
- All employee Gsuite identity require password complexity and MFA.
- Access and device logs are kept and can be used to investigate any suspicious activity.
- Employee accounts are suspended within 24 hours of an employee termination
- A limited number of employees have Gsuite administrative access.

Physical Security

- Descartes Labs has also implemented protocols to secure the Descartes Labs offices and areas within our offices that contain sensitive information. Physical access to our office suite is restricted to badged employees. All Visitors must be registered and escorted at all times.

Privacy

- At Descartes Labs, it's our policy to limit the volume and scope of personal information we collect. Our default approach is to obtain anonymized datasets whenever possible. Where it's necessary to collect personal information, we limit our collection to what's necessary to accomplish our legitimate business purposes.
- The Descartes Labs Platform is hosted by our cloud service providers, with primary storage located in the United States. We maintain internal policies and procedures that set standards for how we process personal information. We follow the Fair Information Practice Principles ("FIPs") and the principles of Privacy by Design ("PbD") in developing, providing, enhancing, and improving our Platform services.
- We maintain transparency by providing a public-facing Privacy Notice on our website that describes our privacy and data protection practices. We honor and respond to individual data rights as required under applicable laws.

1704 B Llano #403, Santa Fe NM, 87505 | www.descarteslabs.com