Overview

Building a platform with strong security requires a holistic and systematic approach.

Our program includes the governance controls to ensure that the platform, data, and code are secure and monitored.

We've adopted a set of policies aligned to NIST 800-53 and NIST CSF to develop a comprehensive security program.

Data Protection

In many cases, we utilize your data sources and you continue to control access and maintain the protections you already have in place.

When your data is accessed, it is encrypted in transit and processed by the platform in memory and not copied to disk. Any data that is stored, such as query results, is encrypted at rest with strict access control.

The table below outlines our platform security features. A complete summary of Datadistillr's security program and corresponding policies is included in the pages below.

- All user access is protected through strong application authentication
- A front-end firewall blocks unauthorized ports and protocols
- Customer instances and data are logically separated
- Access to data sources, queries, and query results is logged and can be audited
- We will undergo a SOC 2 audit by Q3 2022
- Platform can be integrated using your authentication model for user access
- DataDistillr administrator and support access is protected through MFA
- We have a fully tested Business Continuity Plan and offer a 99.9% uptime SLA
- All third party vendors and contractors are fully vetted

- Data source credentials are encrypted and stored in a secrets manager
- Data source access can be whitelisted to ensure requests are coming from the DataDistillr platform
- Data is encrypted at rest
- Data transfers to/from the platform are encrypted
- Queries are scanned for malformed or suspicious content
- Query results are encrypted at rest
- Access to data sources, queries, and query results is restricted. Customer instances and data are logically separated
- User access is logged and can be audited
- Network vulnerability scans are performed quarterly
- A third party executes an annual penetration test

Platform Security

This is a list of security assertions that should be vetted and discussed before inclusion.

DataDistillr Security Program Overview

DataDistillr is deeply committed to security and privacy. Our goal is to make sure you have the information you need to feel confident in our ability to provide you with a secure platform. Additional information about DataDistillr's security program can be provided upon request.

Security Program and Structure Security Policy

DataDistillr's security policy establishes its position on a range of security-related topics. While executive leadership is accountable for the execution of the program, the entire company works diligently to ensure that the security of our customers comes first. Our policies reflect our commitment to providing a trusted solution.

We understand that security due diligence includes reviewing company policies. While it is our policy not to share or distribute the DataDistillr Security Policies, we are happy to share a summary, which reflects all topics covered in DataDistillr's data security program, and answer questions about its contents. The Security Policies themselves are internal documents containing confidential information on how we secure our customer's data and conduct business operations.

Alignment with NIST 800-53

DataDistillr aligns its information security program to the NIST 800-53 framework. Maturation of the information security program is driven by alignment to this framework and an understanding of any potential or evolving threats.

Independent Third Party Review

DataDistillr has partnered with independent security resources to ensure it is properly executing its security program. We believe that consistent monitoring of our platform through regular vulnerability assessments and penetration tests along with review of our policies, vendor management, and risk management programs is critical for our information security program. We rely on our relationships with security, compliance, and governance partners to ensure DataDistillr is held to the highest standards.

Security Training

DataDistillr's Security Training is a mandatory requirement for all employees. The training is structured to educate employees on the Information Security & Privacy Policies, provide an understanding of security in the context of our service and industry, instill the commitment to protect the security needs of our customers, and most of all, to ensure the safety and security of our customer's data.

Application Security

Application security is particularly important, because with applications running in the cloud, we know our cloud partner is responsible for infrastructure level security; but we, through their Shared Responsibility model are responsible for our application security. To ensure that DataDistillr follows best practices for application security, we train on the OWASP Top 10 and perform code reviews for security.

Data Encryption

DataDistillr secures all data in transit via TLS. Systems are configured to require the TLS protocol, meeting industry standards for externally facing systems. You can view an up to date assessment of our TLS configurations by visiting SSL Labs SSL Test.

Symmetric encryption (AES-256) is used to protect data at rest. This ensures that data is only viewable by authorized users.

Data Access

DataDistillr's environment is highly-restricted by design. Access controls are in place to ensure that data is only available to appropriate parties. Internally, DataDistillr employees may be granted access to the DataDistillr platform for administration purposes only.

Data Processed by DataDistillr Technology

To get the full benefit of the DataDistillr technology platform, our partners must share very detailed and potentially regulated data. We realize and understand that this is sensitive information and take our obligation to protect your data very seriously. All personal data is encrypted in transit and at rest in our systems.

Security Policy Summary

The following summarizes DataDistillr's Security Policies. It is our policy not to share our security policies to ensure that we do not inadvertently disclose details that might be relevant to an attacker. This document is intended to be detailed enough to provide insight into our policy framework, which is based on NIST 800-53, without inadvertently disclosing details. It is intended to be shared.

Please direct any questions to security@datadistillr.com.

Master Security Policy - Security Roles and Policies

- List of Required Policies Responsibilities
- Approval Process
- Update Process
- Consequences for Violation
- Standard Tracking Data for Policies Exception Process

Acceptable Use Policy - Use of Company Resources

- Access To Data
- Use of Personal Devices
- Use of Company Devices
- Use of Cloud Resources
- Sharing Documents

Application Security Policy - Software Security

- SDLC
- Licensing
- Code Review

- Required Penetration Testing
- Change Control
- Third Parties

Asset Management Policy - Tracking Assets

- Tracking Assets - Servers, Laptops, Phones, Keys, Licenses
- Process for New and Retired Assets

Business Continuity Policy - Availability, Capacity, and Recovery

- System Capacity
- Contingency Planning
- System Availability - Including Required Plans
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for Critical Systems

Data Classification - Types and Handling of Data

- Classification Tiers (Restricted, Internal, Public)
- Examples of Data in Each Tier
- Handling requirements by Tier
- Encryption Requirements (Simple version: AES-256, RSA 2048, TLS 1.2+)
- Data Handling and Labeling

Identity and Access Management Policy - Authc and Authz

- Provisioning and Deprovisioning Users
- Access Control - Least Privilege
- Authentication - Password Complexity, MFA, SSO Auditing

Incident Response Policy - How we respond to an incident

- Handling Process
- Tracking Process and Required Tracking Data
- Training
- Communications
- Readiness - Contacts

Network Security Policy - Segmentation and Scanning

- Internal Network Segmentation
- Port Status
- Remote Administration
- Integration with Third Party Systems
- Wireless
- Vulnerability Scanning

Partner Security Policy - Defines Partner / Vendor Review

- Vendor Management Program
- Supply Chain Risk
- Tracking
- Review

Physical Security Policy - Office and Data Center Safety

- Clean Desk
- Data Centers Security

- Environmental Controls
- Physical Security Controls
- Required Offices - Company, Shared, Home

Privacy Policy - Privacy Handling

- How Private Data Will Be Handled
- Considers GDPR and CCPA
- Processes for Identifying, Updating and Deleting User
- Data Website Privacy - Cookies and Tracking

Risk Policy - Risk Identification and Management

- Active Risk Identification and Tracking
- Risk Register
- Audits
- Threat Intelligence
- Laws, Regulations and Compliance

Systems Security Policy - Defines Patching and Hardening

- Hardening Guidelines
- Patching for Endpoints and Servers Critical Patches
- Mobile Code