



Automate Your Data Security and Governance Controls

Automate, Govern, Secure: Protect Your Data with Dasera

Dasera secures sensitive data no matter where it lives by finding, flagging, and fixing data risks automatically and continuously so security teams can proactively prevent breaches and data teams can have high quality and usable data.

Dasera goes beyond just Data Security Posture Management (DSPM) to truly secure your data. Continuously and automatically, all your data is classified, tagged, and flagged for risks related to data infrastructure, data attributes, data users, and data usage. Security risks can then be automatically fixed using policy workflows.

“Before Dasera we would take up to 2 weeks to answer certain data-related and data security-related questions, with Dasera it takes us 5 minutes.”



Why Choose Dasera: Reduce Data Security Risks

Dasera helps you protect and govern sensitive data and user access for a secure environment.



Discover Anything, Anywhere

Structured or unstructured, cloud or on-prem, Dasera has you covered resulting in a true single pane of glass.



Data-In-Use Monitoring

With exclusive IP, Dasera is the only data security platform to deeply analyze data usage and correlate results for unmatched risk visibility.



Data Breach Prevention

With Dasera's powerful policy engine and its risk analysis capabilities, Dasera can help avoid damaging data breaches.



ORACLE



Google Cloud Platform



heroku



databricks



SAP



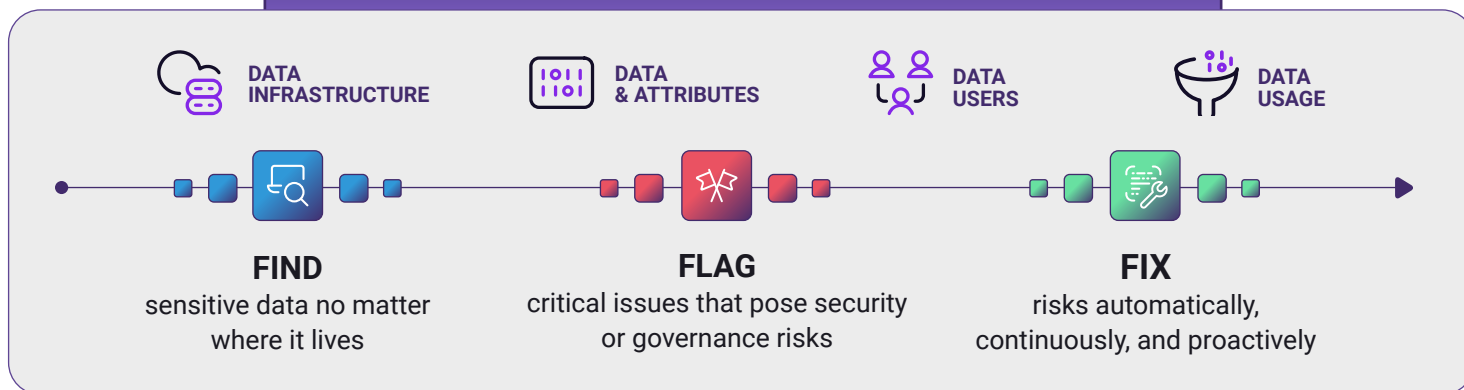
snowflake



Microsoft SQL Server

www.dasera.com
info@dasera.com

Continuous Data Protection Throughout the Data Journey



Sensitive Data and Data Attributes

Discover, classify, and tag sensitive data in newly created data stores



User or Application Access and Privileges

Discover which employees and applications have access privileges to sensitive data



Data-in-Use Monitoring

Ingest all SQL queries used by Users and Applications and analyze for security and compliance risks



Misconfiguration Risks

Identify when sensitive data is not encrypted or publicly exposed



Over-Privileged Risks

Identify when un-sanctioned or stale users have access to sensitive data



Exfiltration and Privacy Risks

Identify queries returning high volumes of data targeting individual sensitive information or modifying critical information



Notify Stakeholders

Alert key individuals of security and data risks



Automatically Remediate

Integrate with 3rd party tools and trigger workflows to automatically handle and rectify security vulnerabilities



Your **responsive** partner in automating data security and governance.

Request a demo at: www.dasera.com/demo

