A FOUR STEP FRAMEWORK FOR PRACTICAL DATA CENTRIC SECURITY

TRUSTLOGIX

A FOUR STEP **FRAMEWORK FOR PRACTICAL DATA CENTRIC SECURITY**

THE CLOUD DATA PROBLEM

Digital Transformation (DX) is fundamentally changing how organizations engage with their customers, partners, and other constituencies. It is now core to the strategy of most organizations and those that do not embrace it risk losing ground to their competitors.

Data is the fuel for this DX wave, and companies rely on being able to rapidly analyze massive quantities of data to power their strategic DX initiatives. This almost always entails moving key datasets to cloud data platforms including Snowflake, Databricks, and AWS solutions such as Redshift and DynamoDB.

This mass exodus of corporate data to the cloud creates a number of security and governance challenges that organizations need to tackle in order to safely execute their DX initiatives. The fragmentation of the organizational data layer across disparate cloud platforms makes it difficult for a Chief Information Security Officer (CISO) or Chief Data Officer (CDO) to answer fundamental questions such as:

WHO IS ABLE TO ACCESS MY DATA?

ARE THEY ONLY DOING SO USING SANCTIONED TOOLS?

IS ANY OF MY DATA UNPROTECTED?

ARE MY POLICIES BEING ACCURATELYFOLLOWED ACROSS ALL CLOUD PLATFORMS?

AM I IN COMPLIANCE WITH HIPAA, GDPR, CCPA, PCI, AND SARBANES-OXLEY?

IN THIS EBOOK, WE LAY OUT A PRACTICAL FRAMEWORK FOR ORGANIZATIONS TO ACHIEVE DATA-CENTRIC SECURITY.

1

OBSERVE & LEARN

2

RECOMMEND & ENABLE

3

CONTROL & PROTECT

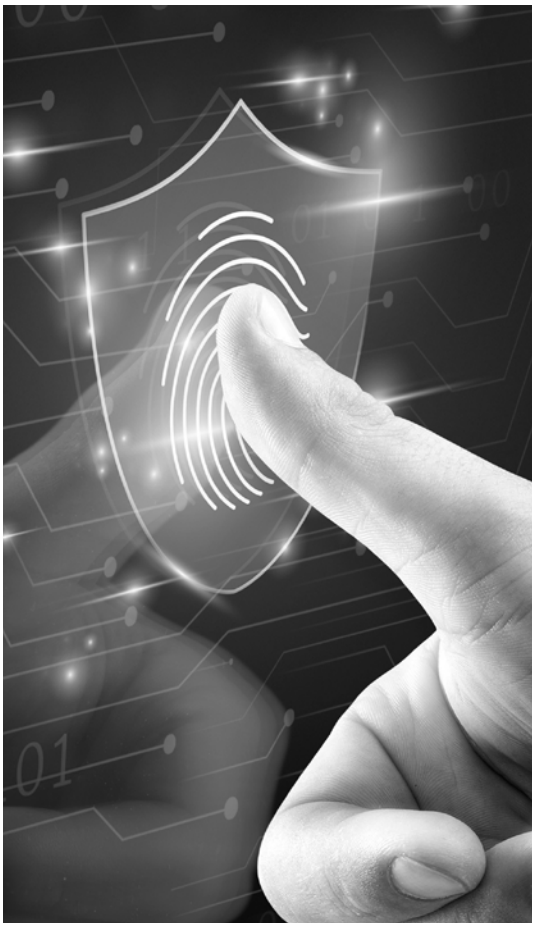
4

AUDIT & RECERTIFY

Using simple and achievable steps, this model will strengthen your security posture while giving your data teams the speed and flexibility they need to monetize your data and propel your business forward safely.

STEP 1: OBSERVE & LEARN

As the saying goes, measure twice and cut once. The first step in your journey is to understand what data has already been shifted to the cloud, if and how it is being used, and by whom. Getting your arms around this information will be powerful in many ways.



- **Monitor data usage patterns:** See how the data you already have out in the cloud is being used and by whom. You can gain insights into which data is most commonly used, which data is most valuable (used by your most strategic projects), and which data is being accessed rarely or not at all.

- **Spotlight data misuse:** Identify patterns where datasets are being accessed off-hours, downloaded at inappropriately high volumes, or accessed in other ways that fit patterns of malfeasance and misuse.

- **Discover dark data:** These are the pernicious data sets that have been moved to the cloud but aren't being used. At best they represent storage costs that can be recouped. At worst they are an unnecessary threat surface that you're exposing. Ideally, they represent ways for you to go back to the business with untapped monetization opportunities.

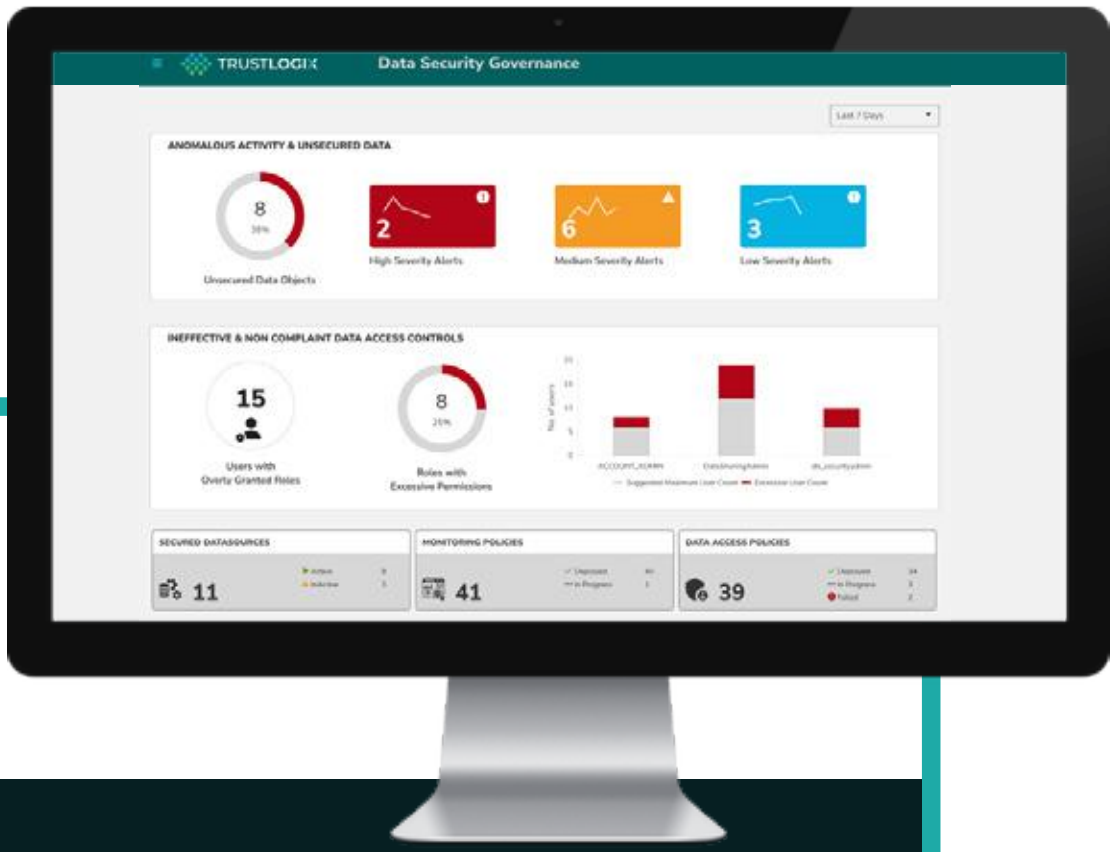
- **Identify Blind Spots:** Discover risk areas that slip through the cracks because they don't get caught by traditional risk management controls. Look for overly granted access to data, abuse of highly privileged roles, sensitive data sharing with 3rd party accounts, and data exfiltration through unapproved usage of client tools,

ACTION ITEMS:

- 1. Take stock of your cloud data stack: Work with your IT operations team to determine what cloud data repositories your organization is using (e.g. Snowflake, AWS Redshift, Databricks, etc.).
- 2. Ensure that someone on your team understands the best practices for those respective tools including privileged access, cryptographic key management, and how to implement fine-grained access controls.
- 3. Understand and document which datasets are being stored in which repositories. Crucially, identify the Data Stewards who own the different datasets.
- 4. Dig into data usage: Determine which datasets are being accessed, how frequently, and by whom. Understand the underlying constructs and rule syntax that defines who (individuals and roles) is allowed to access what data. This will help you determine data usage patterns that you will later verify with the data stewards.
- 5. Inventory the various tools and clients that are being used to access data within your environment.

- **How TrustLogix Can Help:** TrustLogix can quickly and non-intrusively gather much of this information in the background. It deploys quickly and there is no impact to data access performance or privileges and the process is completely transparent to your staff and to data consumers. There are no proxies or agents so business continues to operate smoothly while we catalog your current cloud data operating environment.

LEARN MORE ABOUT TRUSTLOGIX'S NON-INVASIVE ARCHITECTURE



STEP 2: RECOMMEND & ENABLE

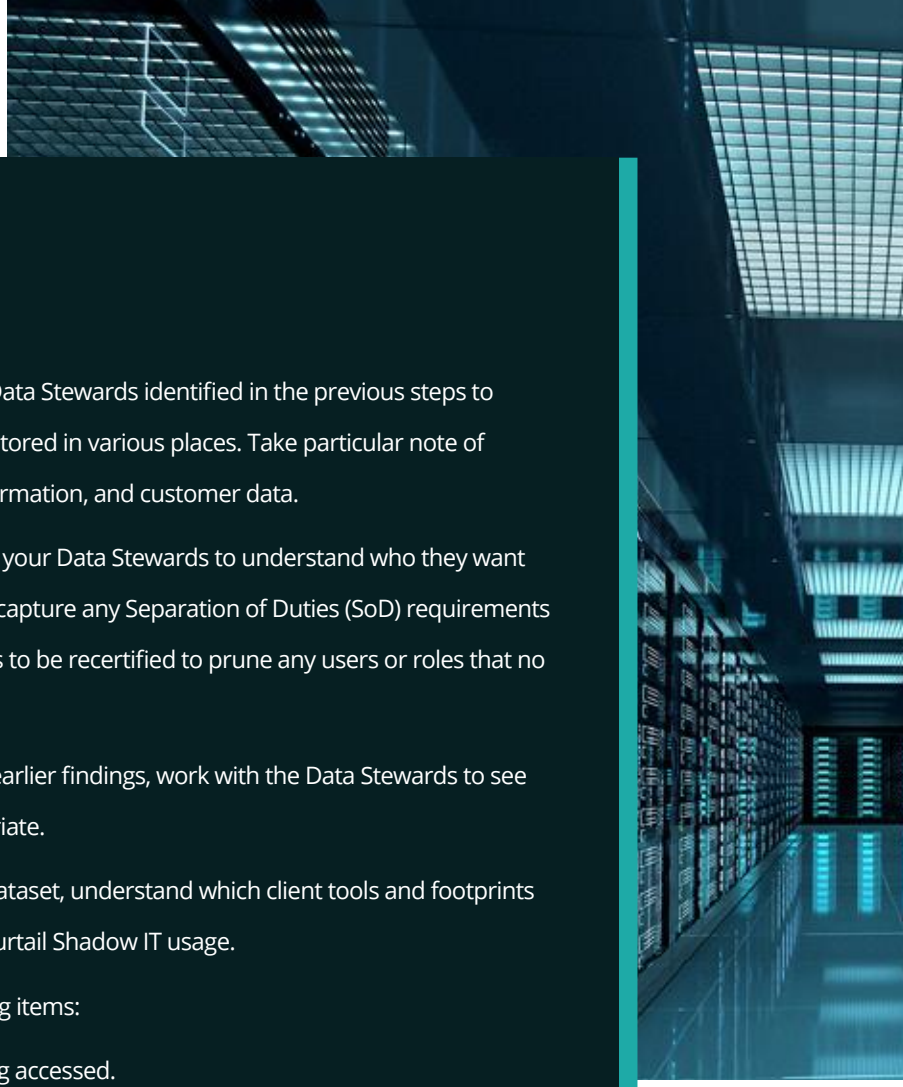
Once you know what data is out in the cloud and how it's being consumed, you need to figure out how much of that is appropriate and how much isn't, and codify appropriate business level access policies. You also need to ensure that the underlying security controls for each of your cloud data repositories are appropriately aligned with the sensitivity of the data they store. The specific goals for this step in the framework are:

- **Eliminate Dark Data:** Review data consumption with your Data Stewards and discuss datasets that are being completely ignored or accessed very infrequently. These could represent a business opportunity by notifying consumers that the data is available for their use. If it's not needed, it can be removed from your cloud to reduce cost and risk.

- **Curtail Shadow IT:** Review the various clients and tools that are being used to access your data with the appropriate Data Stewards. Understand which tools are sanctioned and work with your IT team to block any unsanctioned "Shadow IT" tools which could lead to security risks, compliance issues, data exfiltration, malicious usage by insiders, and license violations.

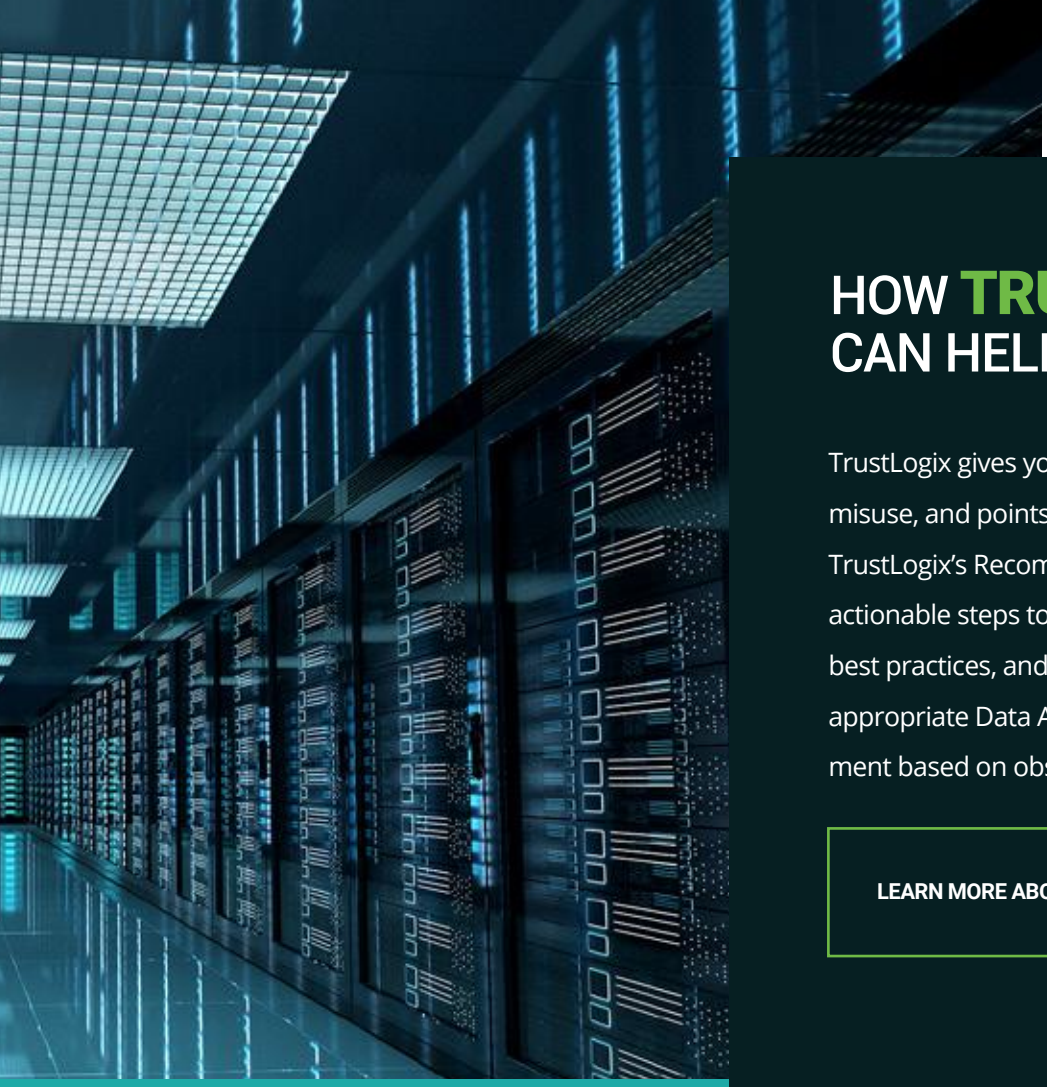
- **Define Access Control Policies:** Define proactive Data Access Control policies based on your learnings so far. These policies need to be as fine-grained as the data sensitivity mandates, and multi-faceted as we explain below.

MORE DETAILS ON WHY THIS STEP OF THE FRAMEWORK IS IMPORTANT IS COVERED IN OUR BLOG IDENTIFY BLIND SPOTS IN YOUR CLOUD USING DATA-CENTRIC SECURITY



ACTION ITEMS:

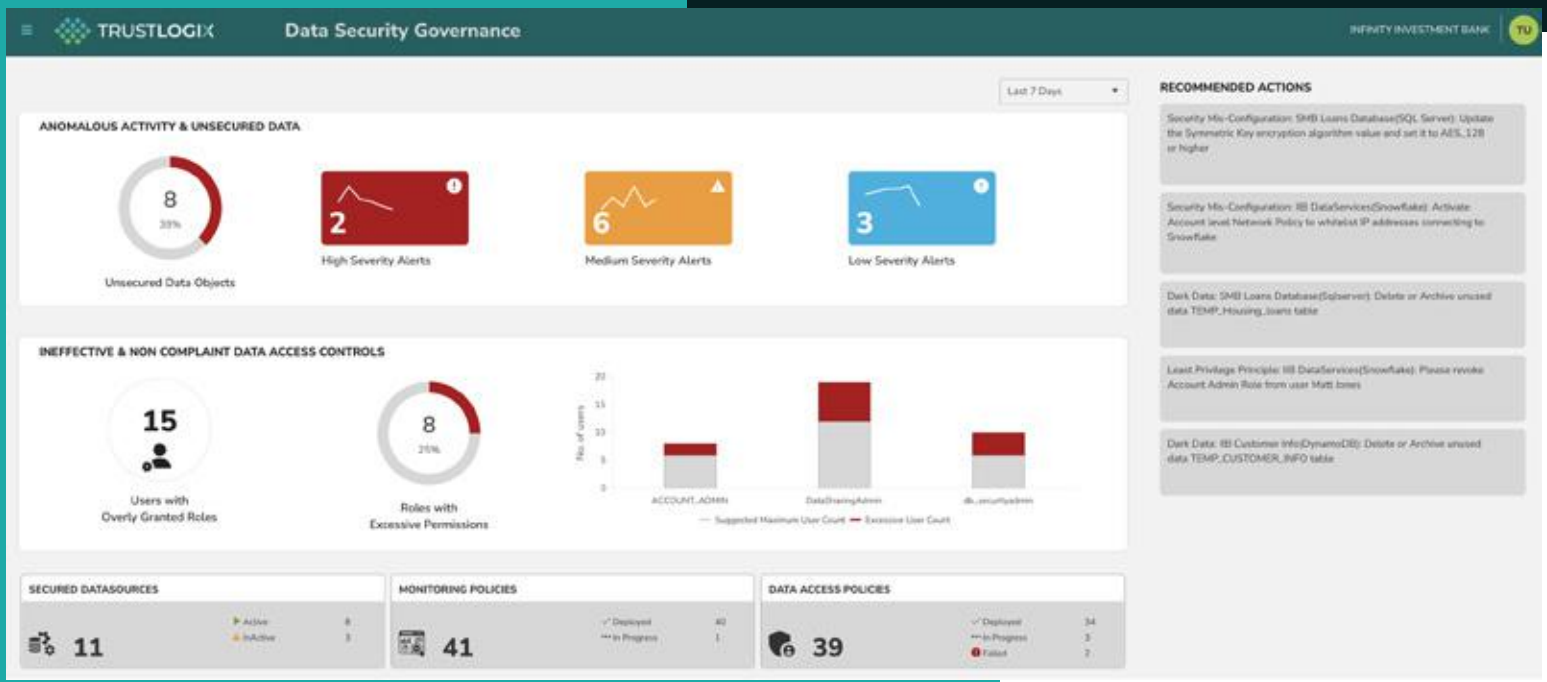
- 1. Inventory your data: Work with the Data Stewards identified in the previous steps to catalog which types of data are being stored in various places. Take particular note of sensitive data such as PII, financial information, and customer data.
- 2. Define "Appropriate Use": Work with your Data Stewards to understand who they want (and don't want) using their data. Also capture any Separation of Duties (SoD) requirements as well as how often data access needs to be recertified to prune any users or roles that no longer need access to the data.
- 3. Validate data usage: Based on your earlier findings, work with the Data Stewards to see which data usage is and is not appropriate.
- 4. Specify Sanctioned Tools: For each dataset, understand which client tools and footprints are allowed to access that dataset to curtail Shadow IT usage.
- 5. Create a "Danger List" of the following items:
    - a. Dark Data: Data that is not being accessed.
    - b. Overly Granted Policies
    - c. Ineffective policies
    - d. Unprotected data
- 6. Based on this new contextual understanding of your datasets, define a set of fine-grained access control and infrastructure policies. Create a policy for each of your datasets that encapsulates the following:
    - a. Define roles that have common meaning across your business and tech stack
    - b. Ensure that sensitive data is being encrypted in the strongest way possible
    - c. Specify which users and roles are allowed to access the data down to the row and column level, including masking and other rules as required.
    - d. Create Monitoring Policies that look for suspicious behaviors that could indicate data exfiltration is taking place
    - e. Specify a list of authorized client tools that are permitted to access the dataset



HOW TRUSTLOGIX CAN HELP:

TrustLogix gives you fast, deep insight into dark data, data misuse, and points of vulnerability for your cloud data. TrustLogix's Recommendation Engine provides you clear and actionable steps to clean up excessive privileges, implement best practices, and identify data misuse. It also recommends appropriate Data Access Control policies for you to implement based on observed data usage patterns.

LEARN MORE ABOUT TRUSTLOGIX RECOMMENDATIONS HERE.



STEP 3: CONTROL & PROTECT

Now it's time to put the learnings from Steps 1 and 2 into action. This step in the framework is about enforcing access controls while empowering your Data Consumers and without slowing down the speed of business.

ACTION ITEMS:

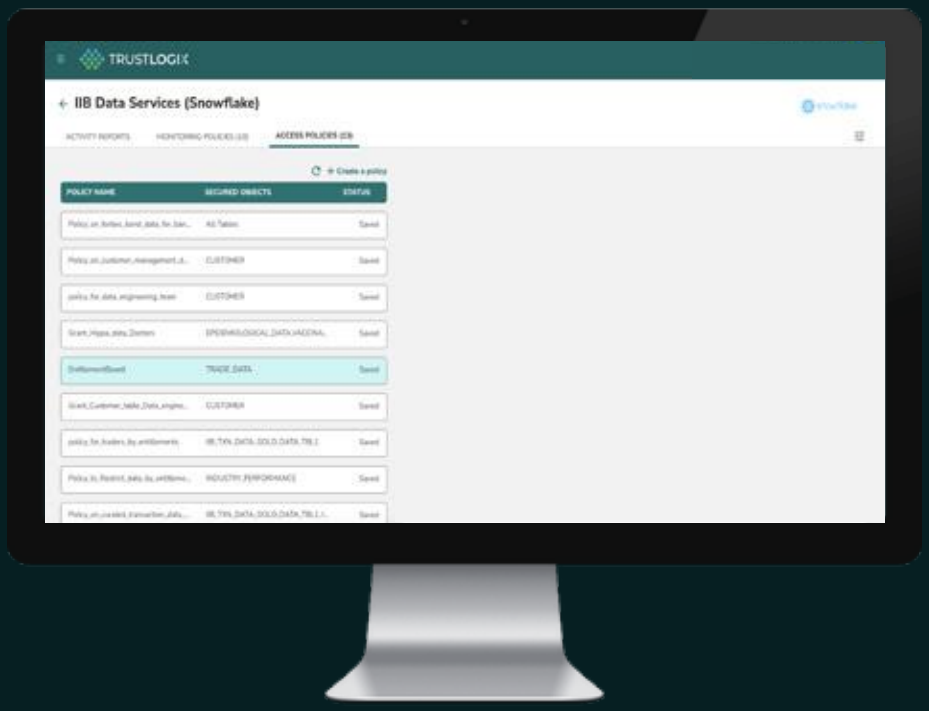
- 1. Work with your IT staff to take corrective action on the "Danger List" you created in Step 2 including
    - a. Strongest practical encryption for sensitive data
    - b. Align privilege levels for various roles with best practices
    - c. Reduce the number of over-privileged users
    - d. Implement appropriate network level controls to prevent unauthorized clients (Shadow IT) from accessing various datasets
- 2. Work with your Data Stewards to implement the data authorization policies mapping the roles you defined in Step 2 with specific fine-grained data entitlements that will dictate who is authorized to use each dataset and under which constraints
- 3. Ensure that your IT staff models the appropriate fine-grained controls based on the constructs and rules native to each cloud repository. A source dataset may end up in two different platforms (e.g. Snowflake and Databricks) so the original policy will need to be implemented in each of those platforms using their native syntax and toolsets.

HOW **TRUSTLOGIX** CAN HELP:

TrustLogix empowers your Data Stewards and Data Operations teams to collaborate by providing a unified control plane for Data Security Governance. Data Stewards can define business policies using roles and business terms to specify who they want to have access to their data. Data Operations can use TrustLogix to model those policies at a very fine-grained level and TrustLogix will then interface with your various cloud data platforms to to translate those policies into platform-specific rules for Snowflake, Databricks, Redshift, and the various other elements of your cloud data stack.

This delivers several important benefits for your organization:

- **1.** It saves your Data Operations team time from having to manually define redundant policies for each new dataset. They can leverage existing TrustLogix policies and apply them to new datasets as needed.
- **2.** Your policies are applied correctly and consistently across your infrastructure. Your Data Operations team no longer needs to understand the security controls across your heterogeneous cloud services in deep detail. TrustLogix is able to “translate” a common policy into service-specific constructs and interface with those various services to apply policies as needed.



STEP 4: AUDIT & RECERTIFY

This is the final step in each iteration of applying this framework. At this point you should be in a good steady state where you have solid controls around the operational infrastructure for your cloud data. You now need to demonstrate that your policies have been implemented properly and are being correctly followed by the organization.

This is important for two reasons:

- **Security:** Data access needs are guaranteed to evolve over time as project teams evolve, initiatives change focus, organizational structures change, and so on. It is imperative that you periodically re-certify that your data access control policies are up-to-date and being correctly followed to ensure that your controls remain appropriately aligned with the business.

- **Compliance:** As or more importantly, you will face compliance mandates for privacy and security legislation including GDPR, PCI, HIPAA, and CCPA. In addition, Sarbanes-Oxley (SOX) mandates that access to information that will materially affect the business be periodically reviewed and attested to by any publicly traded companies.

ACTION ITEMS:

- 1.Audit how each of your datasets was accessed and cross-reference those results against the policies that were modeled in Step 2 and implemented in Step 3. Use the reporting capabilities of your cloud data services to generate and store audit reports that demonstrate compliance.
- 2.Meeting with your Data Stewards to recertify that your data access control policies are still up-to-date. Document any changes to policies if needed and notate the date of the recertification.
- 3. Deprovision any users or roles that no longer need access to specific datasets due to changes in business requirements or user roles.

HOW TRUSTLOGIX CAN HELP:

Audit and Compliance recertification is typically very possible in almost any operating environment, but is challenging because it can be extremely resource and process intensive. TrustLogix automates most of this effort with many key capabilities:

- **1.** Detailed audit and access reports including SoD violations, overly granted access, unused datasets, etc.
- **2.** Automatic notification of recertification steps to incumbent governance systems such as SailPoint.
- **3.** Centralized console to prune access to specific users and roles and take other remediative actions

CONCLUSION

Chief Digital Officers and Chief Information Security Officers are faced with a daunting challenge. They need to make organizational data accessible to various Data Consumers by making it available on popular cloud data platforms such as Snowflake, Databricks, AWS Redshift and others.

At the same time, they are the ultimate stewards for safe-guarding that data and ensuring that it's used appropriately, without betraying customer trust and in line with compliance mandates including GDPR, CCPA, PCI, HIPAA, and SOX (Sar-banes-Oxley).

This four step Data Centric Security framework is a practical roadmap that empowers CDOs and CISOs to achieve this tricky balance of keeping their organizational data safe and secure and meeting compliance mandates, all without slow-ing down their Digital Transformation initiatives.