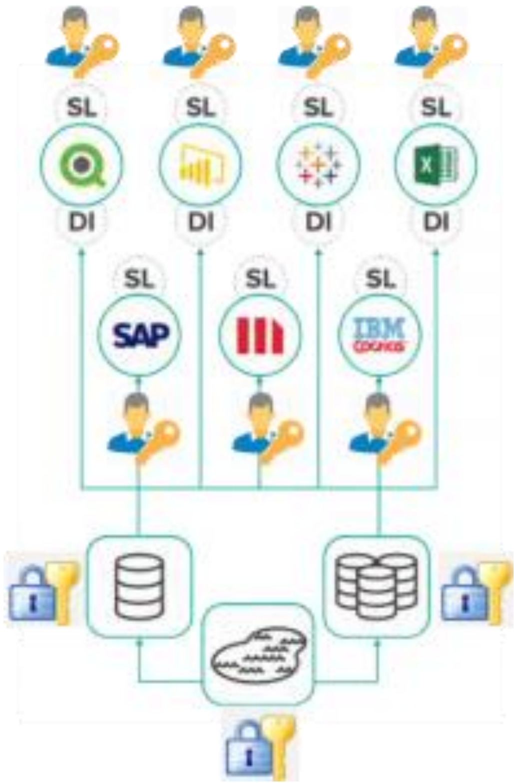
Incongruent Security & Governance Policies Across Enterprise Reporting Services

- Security and Access Management
- Incongruent security policies across datasets and databases
- Manage Security leakage with BI Tools

- Sophisticated security and governance policies
- Single data interface
- Use LDAP or Active Directory Infrastructure
- Delegated Authorisation for BI tool or applications
- Secure data at rest

Challenges

One of the biggest challenges businesses face within the data and reporting realm is security and access management. These days organisations have regulatory requirements to audit and monitor their reports to understand “who”, “what” and “when” data was accessed. Every time BI teams work with data sets across multiple, siloed databases, each with their own security policies, they are opening their organisation to risk. It’s often too complicated for the end user or a business user to understand who should be able to access the report. In addition to that organisations also need to manage security leakage when utilizing connection pools for BI tools or largely depend on security aggregation systems.



Solution

It's imperative for organisations to secure data and have sophisticated security and governance policies. Improving performance, agility, and the return on investment in analytics is important, but means nothing if data is not properly secured and governed. Instead of distributed security protocols, an enterprise should consider using a single data interface, no matter where the data is stored. Enterprise should also enable self-service access to curated data sets without the risks associated with data movement and the complexity of integrating a myriad of security and authorization protocols. Manage all your users and groups using your existing LDAP or Active Directory infrastructure. Use delegated authorization for any BI tool or custom application. Enterprises should aim to secure data at rest using data-platform-level encryption zones and masking data based on user access and permissions. Dedicated roles and security groups should be created for administrators, designers, query users and more.

How AtScale can help

AtScale’s security and data governance capabilities leverage a company’s best security practices and add another layer of capabilities to ensure data security. AtScale’s adaptive analytics fabric also mitigates risk by checking security requirements at the source databases and applying those requirements to query results.

User identities are considered, even when accessing data through a shared connection pool, and security policies from all data sources are collected and merged to filter results appropriately. These same security policies are applied to data aggregates, eliminating unintentional exposure of restricted or private data. AtScale provides a host of security and governance capabilities such as end- to-end Transport Layer Security (TLS) and support for the LDAPS secure protocol. AtScale complies with the JWT, CORS, and REST standards for API security, and AtScale’s Acceleration Structures eliminate data copies and opportunities for data exploits.

Access to raw data is managed by AtScale’s patented True Delegation technology. True Delegation satisfies the most stringent data governance and access auditing policies by preserving user-level access controls when querying the underlying data platform using delegated authorization. In addition, user access permissions are applied to every row and column of the data being queried, ensuring no data is returned that the user is not authorized to access.