ThoughtSpot

WHITE PAPER

ThoughtSpot Cloud: Comprehensive Data Security for Analytics

Introduction

As more workloads move to the cloud - Gartner says 45% of IT spending on system infrastructure, infrastructure software, application software, and business processing outsourcing will shift to the cloud by 2045 - the conversation has shifted. The questions no longer are, “What is the cloud, and how can we benefit from it?” Rather, the questions are now, “How do we ensure data and application security in the cloud?”

Cloud platforms have an excellent track record regarding data security. They are built with security controls around access, authentication, and authorization, data protection through encryption and other mechanisms, as well as sophisticated auditing and monitoring capabilities.

For example, AWS, the largest cloud platform by market share, says it “regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor” to meet security and compliance standards for finance, retail, healthcare, government, and more.

So for those organizations looking to deploy enterprise applications on top of these platforms, the question then becomes, “How do solutions such as ThoughtSpot Cloud that run on these platforms ensure data security at the application layer?”

Maximum Security with ThoughtSpot Cloud

We built ThoughtSpot Cloud with data safety and security fundamental to and inherent in its architecture, as the application engages with both the cloud infrastructure layer and the data layer. The ThoughtSpot analytics cloud relies on two key pillars to ensure data security:

- Minimize data received, and
- Minimize risk of data loss

ThoughtSpot Cloud intentionally capitalizes on the power, elastic scalability, and centralized governance of the investments you have made in your cloud data warehouse, while unlocking the value of that data for your business users. Features of ThoughtSpot Cloud, as well as operating principles of ThoughtSpot the company, are highlighted in the following sections.

System Design

ThoughtSpot designs its hosted data analytics SaaS platform system to meet its regulatory and contractual commitments. These commitments are based on the services that ThoughtSpot provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that ThoughtSpot has established for its services. ThoughtSpot establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in ThoughtSpot's system policies and procedures, system design documentation, and contracts with clients.

Processes and Procedures

Management has developed and communicated processes and procedures to their employees to ensure the execution of policy documentation and critical business processes. Changes to these procedures are performed annually and are authorized by management. These cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from the proposed security approaches
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access

- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response

ThoughtSpot maintains a process for reviewing and updating security policies on an annual basis, and employees must complete annual security awareness training. The Director of Information Security is responsible for creating and maintaining information security policies, which are reviewed and updated at least annually. The documents and policies reviewed during the audit period include the following:

- Acceptable Use Policy
- Access Control Policy
- Application Security Report
- Asset Management Policy
- Background Check Policy
- Backup Procedure
- Business Continuity Plan
- Change Management Policy
- Cloud Subscription Agreement
- Code of Conduct

Application Development

ThoughtSpot maintains a Software Development Lifecycle Policy that establishes standards for secure software development. Per policy, the organization follows OWASP security guidelines, and all development or acquisition projects, as well as modifications, are reviewed to mitigate potential security risks before being placed into production. All developers are trained in secure coding techniques, and Veracode penetration tests and vulnerability scans are used to test against the OWASP Top 10.

Authentication and Authorization

- **Zero-trust policies** - Multiple services monitor, detect, and protect against common attack vectors.
- **Tenant isolation** - Fully isolated tenants prevent data leakage and provide protection against unauthorized ccess.[1]
- **Authentication** - ThoughtSpot supports multi-factored authentication, and ThoughtSpot Cloud integrates with a number of identity providers via SAML.
- **Activity audit logs** - User login and activity logs are secured and available to administrators.

- **ThoughtSpot Administrator access** - Access privileges of ThoughtSpot employees are based on job r equirements, using the principle of least privilege access, and privileges are revoked upon termination of employment. Entitlements are reviewed semi-annually.[2]
- **Support control** - ThoughtSpot is here to support you however you need. You control the level of access you want to provide to our support team, as well as the way in which you would like to engage us. Visit our ThoughtSpot Support page to learn more.
- **Data replication** - ThoughtSpot Cloud does not copy data. All data remains in your cloud data warehouse. Note that indexing for an enhanced search experience will store distinct values from the searchable columns in the data to which you connect, along with relevant metadata such as column names and row-level security rules, in an in-memory data store.
- **Analytics at the source** - Your data remains in the data warehouse of your choice, and queries are performed l ive in-database. There is no data movement required.
- **Customer-specified indexing** - Tokens are helpful for guiding users' search experiences, but are not required for full functionality of ThoughtSpot Cloud. You control whether data is tokenized at the table, worksheet, and column level. ThoughtSpot can provide commands to prevent any data indexing.

Data Security

- **Data encryption** - ThoughtSpot Cloud provides comprehensive support for data encryption at rest and in transit, leveraging AES 256-bit encryption and keys unique to each customer for encryption-at-rest, and TLS 1.2 for encryption-in-transit.
- **Security passthrough** - ThoughtSpot Cloud enables security passthrough for supported cloud data warehouses, enabling you to leverage existing policies from your cloud data warehouse.
- **AWS cloud infrastructure** - ThoughtSpot Cloud runs on the industry's most secure cloud infrastructure in AWS.
- **Data governance and secure sharing of data** - Granular object-, table-, column-, and row-level access rules control what users are permitted to see. Privileges determine what actions users can perform.
- **Account termination** - All data along with the tenant instance is deleted upon termination or expiration of the agreement or order form.
- **Partnership** - Security is a partnership between the provider and customer, both with specific responsibilities. ThoughtSpot provides its customers with extensive capabilities to configure their instances to meet their own security policies and requirements. However, overall security responsibilities are shared between customers, ThoughtSpot, and the data center provider.

[1] ThoughtSpot trial accounts are isolated by user groups.

[2] ThoughtSpot trial accounts do not receive admin access to their account, and can contact ThoughtSpot Support for more help.

[3] A Microsoft Azure-hosted version of ThoughtSpot Cloud is on the short term roadmap.

Data Backup and Recovery

ThoughtSpot maintains a formally documented Backup Procedure to ensure that backups are completed. The ThoughtSpot Cloud production environment has automated backup procedures for ThoughtSpot tenants. Backup and snapshot capabilities are part of ThoughtSpot services running in each tenant. Daily backups are saved for 30 days. Backups are stored in AWS in object storage (S3), which is available in the same region across availability zones. In addition, ThoughtSpot also takes regular snapshots, which are stored on the disks attached to the ThoughtSpot tenant VM instance.

Per policy, hourly snapshots are kept for four consecutive hours, four-hourly snapshots are kept for six consecutive four hour periods, daily snapshots are kept for seven consecutive days, weekly snapshots are kept for four consecutive weeks. The ThoughtSpot corporate environment uses Druva backup software. Backups are stored in the Druva Cloud service. Per policy, daily snapshots are kept for seven consecutive days, weekly snapshots are kept for four consecutive weeks, monthly snapshots are kept for 12 months, and annual snapshots are taken for servers that are kept for three years.

Risk Assessment Process

ThoughtSpot maintains a Risk Management Policy that defines the process for identifying, responding to, mitigating, and reporting risks. Assets are identified, documented, and sorted into similar categories, and risk determination for each category of assets is performed with risks calculated. The determined risk response takes into account the impact and likelihood of exposure. Risk owners assist in determining the appropriateness of selecting controls that transfer, avoid, or mitigate risk.

Per the Risk Management Policy, risk owners are involved with determining the risk treatment plan, and the response strategy must consider the impact rating and likelihood of exposure. The organization gathers input from different departments to consider the best treatment plans for the highest risks to ensure that the mechanisms to mitigate, accept, or avoid risk are appropriate for the level of risk involved and the sensitivity of the systems.

Compliance & Governance

- **GDPR compliance** - ThoughtSpot is compliant with the European Union's General Data Protection Regulation (GDPR). ThoughtSpot's data processing addendum incorporates EU-approved transfer mechanisms, namely the European Commission's standard contractual clauses. Customers can rely on these protections to transfer EU personal data using our services.
- **HIPAA compliance** - ThoughtSpot is HIPAA compliant and ensures access to confidential data is limited and patient information is protected. A ThoughtSpot Business Associate Addendum is available to execute as needed.
- **SSAE 18 SOC 2** - ThoughtSpot has successfully completed the Service Organization Control (SOC) 2 Type II audit. The SOC 2 report verifies the suitability of the design and operating effectiveness of ThoughtSpot's information security practices, policies, procedures, and operations to meet the standards for security, availability, and confidentiality.
- **ISO 27001** - ThoughtSpot is ISO/IEC 27001:2013 certified.

Conclusion

You have captured a wealth of data in your cloud data warehouse. Search & AI-driven analytics with the ThoughtSpot analytics cloud is the easiest way to deliver value from that data for your business teams and customers. But security of that data - and the rest of your infrastructure and applications - can never be an afterthought.

ThoughtSpot Cloud provides users with a familiar search-based interface for analytics, so they can discover and share the insights they need based on the data in your cloud data warehouse. And with ThoughtSpot Cloud connected to your cloud data warehouse of choice, you can trust that you have introduced no security risks to your data, infrastructure, and applications.