Starburst
ANALYTICS ANYWHERE

WHITE PAPER

Information security at Starburst

An overview of security practices and processes applicable to Starburst, Starburst Enterprise, and Starburst Galaxy.

Overview

Corporate information security policies and procedures

- Roles and responsibilities
- Privacy policy
- Terms of service and license agreements
- Compliance - System and Organization Controls (SOC) 2 Type 2 & ISO 27001
- Risk management
- Change management and change control
- Incident response
- Access control
- Malware management and antivirus
- Multi-factor authentication and remote access
- Security awareness
- Vendor management
- Vulnerability reporting and disclosure

Software development and security practices

- Development methodology
- Penetration tests
- Security and vulnerability management processes

Security and Starburst Enterprise

- Private deployment
- Data sources and transfer
- Data security
- Releases

Security and Starburst Galaxy

- Data sources, catalogs, and clusters
- Control plane
- Authentication
- Logging and monitoring
- Audit and compliance
- Usage information

Resources and contact information

Overview

Starburst is the leader of the open source community around the Trino project. Trino (formerly Presto® SQL) is the fastest open source, massively parallel processing SQL query engine designed for analytics of large datasets distributed over one or more data sources in object storage, databases and other systems.

Starburst provides the Starburst Enterprise and Starburst Galaxy, both based on Trino.

Starburst Enterprise is a fully supported, enterprise-grade distribution of Trino. It adds integrations, improves performance, provides security, and makes it easy to deploy, configure and manage your clusters.

Starburst Galaxy is an easy to use, fully-managed and enterprise-ready SaaS offering of Trino. Configure your data sources, and query your data wherever it lives. Starburst takes care of the rest so you can concentrate on the analytics.

The Starburst team includes experts from the Trino community as well as the wider software development, information security and big data communities. Together we have accumulated hundreds of years of experience in these fields and we are putting our knowledge to work for our customers.

Information security and all aspects around data protection and governance are at the core of many of our activities. We are committed to providing you with secure products and services, and to continual improvement of our information security controls and practices.

Use this document to gain a better understanding of all relevant details about the security practices applicable to Starburst and our products.

Corporate information security policies and procedures

Roles and responsibilities

The information security team at Starburst is responsible for implementing and maintaining organization-wide information security policies, remediating security incidents, and managing risk at an appropriate level for the Starburst organization. The team reports directly to the Vice President of Engineering.

Privacy policy

Starburst is committed to protecting the privacy of individuals who visit Starburst's sites and individuals and companies that register to use or purchase our software or services.

Under certain circumstances, you have rights under international regulations and data protection laws in relation to your personal data. Contact us to exercise any of your rights.

Details are available in our privacy policy.

Terms of service and license agreements

The following terms of service and end user license agreement (EULA) documents are available:

- Starburst Galaxy terms of service
- Starburst Enterprise end use license agreement

Compliance - System and Organization Controls (SOC) 2 Type 1

Starburst has obtained SOC 2 Type 2 compliance for Starburst Galaxy. Starburst is ISO/IEC 27001 certified. Contact us for a copy of the external attestation.

Risk management

Starburst conducts annual risk assessments and manages a risk register, which is reviewed regularly. A risk management program is in place to identify and prioritize risks, and ensure appropriate application of resources to minimize any negative impact.

Change management and change control

Starburst applies a systematic approach to managing change so that changes to services impacting Starburst and our customers are reviewed, tested, approved, and well communicated. Change management processes are in place to ensure changes are tailored to the specifics of each environment. The goal of Starburst's change management processes is to prevent unintended service and business disruptions and to maintain the integrity of services provided to customers. All changes deployed to production undergo a review, testing, and approval process.

Incident response

Starburst requires the identification of and response to suspected or known security incidents; mitigation, to the extent practical, of harmful effects from security incidents that are known or suspected; and documentation of these incidents and their outcomes.

An incident response program is in place and roles and responsibilities are defined for all functions to ensure impact is minimal and cost and downtime is limited to the furthest extent possible. Regular tabletop exercises are conducted.

Access control

Access to confidential data is granted on a need-to-know basis, and only the minimum level of access required to satisfy business needs is granted.

Malware management and antivirus

Crowdstrike is utilized to protect Starburst hardware from legitimate and potential intrusion attempts. The Starburst IT group manages the Crowdstrike tool, and ensures updates are pushed regularly, to minimize malware risk.

Multi-factor authentication and remote access

Okta is used as our single sign-on provider for all business applications that support SAML. This allows us to enforce Starburst's password policy for all of our business applications and two-factor-authentication when logging into Okta and Okta-managed applications.

Security awareness

Information security training is delivered to all employees during their employment at Starburst upon hire and at least annually thereafter.

Vendor management

Starburst requires that all vendors are assessed for their overall security posture.

Vulnerability reporting and disclosure

If you believe you have discovered a vulnerability in a Starburst product, or have a security incident to report, contact us.

Once we have received a vulnerability report, Starburst takes a series of steps to address the issue.

Software development and security practices

Development methodology

The engineering teams, and others involved with software development at Starburst, implement the following best practices:

- Fine grained project management for each feature and bug fix.
- Enforced peer reviews for any changes. Two or more reviewers are activated for more sensitive or complex changes.
- Required automated and manual testing.
- Automated code and dependency scanning for security vulnerabilities.
- Automated release processes.
- User documentation as part of feature delivery.
- Minimized attack surface by reduction of software components included in archives, machine images, and containers.

These processes are in place to ensure quality and identify security vulnerabilities prior to releasing code to customers and into production environments.

Tests may include functionality, compatibility, UI consistency, performance, security, integration, and regression tests as applicable for a particular change.

Penetration tests

Annual penetration tests are conducted by Starburst. Upon request, customers may obtain executive summaries of these tests.

Security and vulnerability management processes

Starburst continuously monitors cloud environments for system vulnerabilities in accordance with formally documented vulnerability management processes and procedures.

Starburst utilizes Veracode to conduct regular static code scanning and library security reviews. Veracode is an industry leader for application security and the platform allows for efficient vulnerability reporting and management.

The platform produces software composition analysis (SCA) and static application security testing (SAST) reports. The reports are reviewed, and identified vulnerabilities are addressed based upon CVE level. Critical risk and high risk vulnerabilities are prioritized for remediation. Each reported vulnerability is verified to be valid and applicable, or a false positive. This analysis includes assessing the code paths, library usage and other aspects. The results of all these tasks are tracked for reference and further analysis as necessary. False positives are configured to not be reported again.

For true positives, the development process includes addressing and remediating any legitimate critical or high level findings. Medium, low and informational vulnerabilities are reviewed and placed into the backlog and scheduled for future sprints, if legitimate, exploitable risk is identified.

Upon your request, Starburst can provide an executive summary of the reports. The reports may be provided once per quarter.

You may conduct your own vulnerability and code scans. Starburst can be notified of any findings. Starburst only addresses and remediates vulnerabilities as identified by the Starburst Veracode instance.

Security and Starburst Enterprise

Starburst Enterprise is a fully supported, production-tested and enterprise-grade distribution of open source Trino.

Private deployment

Starburst Enterprise is deployed entirely within an environment controlled by the customer. This allows you to apply any layers of security based on your unique organizational policies and risk tolerance. This also means that any data sources are completely under your control and you can take any security measures desired to control access from Starburst Enterprise to the data sources. Starburst supports integration with numerous authentication and authorizations and other security related features. Learn more about all these in the security section of the reference documentation.

Data sources and transfer

Since Starburst Enterprise and all data sources are completely within your systems, Starburst does not have any access. Telemetry data about your usage is automatically submitted to Starburst using an end-to-end encrypted connection, but can also be submitted manually.

Your consent is requested, if data is transferred to Starburst as part of a support request, Because it is not required for the service to operate, generally this transaction is classified as a "causal and incidental" transfer of data.

Data security

You can configure Starburst Enterprise to use encryption (TLS/SSL) for all data in transit and at rest. The connections include client tool connections to Starburst Enterprise, cluster internal communication, and access to the configured data sources. No data is stored in Starburst Enterprise. The desired configuration must be implemented and managed by you.

Releases

Starburst follows a quarterly release process for the LTS (Long Term Support) version and we patch these LTS versions regularly. These patches include security and bug fixes, and each patch release is assessed and reviewed by a core review board prior to the work being executed.

New releases and patches are communicated to customers via our account team and are publicly available on our documentation.

Security and Starburst Galaxy

Starburst Galaxy provides the benefits of Trino, on an easy to use, fully-managed and enterprise-ready SaaS platform.

Data sources, catalogs, and clusters

Your data sources for Starburst Galaxy are managed by yourself in a cloud provider infrastructure. The data sources remain under your control. Your data is never stored in Starburst Galaxy. Only queried data is accessed by Starburst Galaxy.

A Starburst Galaxy catalog is configured by you to connect to your datasource. As part of this configuration, you will provide the credentials necessary to access the data source.

These catalogs can be used in one or more clusters. Starburst Galaxy will spin up compute clusters in the same cloud region as your catalog(s). The clusters connect to the catalog using the authorization information provided in catalog creation to connect to your data. Starburst Galaxy uses a different IP address for every cloud region. You can configure your data source to allowlist only the IPs needed by Galaxy. You can find the IP Allowlist in Starburst Galaxy's security documentation.

Access to the Starburst Galaxy user interface, and directly to clusters with clients, is secured with Transport Layer Security (TLS) and globally trusted certificates.

Control plane

The control plane of Starburst Galaxy manages the overall application, provides configuration storage and all other aspects of managing the system for all users. The control plane is deployed and managed by Starburst in our cloud environments. All storage is encrypted and data is encrypted on a per customer basis. Only a limited number of privileged users at Starburst are granted access to the control plane.

Authentication system

Starburst Galaxy provides a hosted login experience allowing users to sign in with standard username and password credentials. You can manage all users for your organization with the Starburst Galaxy user interface.

Authorization system

Starburst Galaxy includes a role-based access control (RBAC) system to support your security needs. It makes it easy to configure the correct access rights to Starburst Galaxy, the clusters, the configured catalogs and the underlying schema/tables from the data sources for every user.

Users are assigned one or more roles. A role has a name, and can be assigned privileges on entities, such as cluster management, user creation, audit log viewing, and others. You can manage users, roles, and privileges in the Starburst Galaxy user interface.

More information is available in the Starburst Galaxy security documentation.

Logging and monitoring

Starburst Galaxy includes comprehensive logging of events and end-to-end user activities.

Audit and compliance

Starburst audits all actions that are taken on your account. Audit logs are maintained within the user interface and are available to you. Query history shows a list of all queries processed on all clusters. It allows you to view, inspect, and filter completed query execution processes. Query history is limited to your role's history unless you are an account admin or your permissions are set to view all queries.

Usage information

Starburst strives to access and collect only the minimum amount of information needed to provide our products and services. Employees with data access undergo regular appropriate use training and our environment is protected with robust security measures and controls.

Resources and contact information

You can find further information about security, governance, risk management, compliance or data privacy in the security documentation: https://docs.starburst.io/security/index.html

Contact for questions and requests:

- General: security@starburstdata.com
- Data privacy: privacy@starburstdata.com.

Starburst
ANALYTICS ANYWHERE