ToogleBox Security Overview

This document gives G Suite administrators an overview of the security features of **ToogleBox**. It explains how **ToogleBox** makes use of the access granted to G Suite domains. As a third-party application of G Suite, **ToogleBox** matches its security standards.

This overview covers both technical and functional security features, and system development practices.

Technical Security Features

ToogleBox technical security is inherited from Google. All services are built and hosted on the Google App Engine (GAE) platform. **ToogleBox** interacts through Google APIs and uses Google Cloud Storage, Google Datastore, and Google Cloud SQL.

All information resides in Google's data centers and protected by Google's Security Model, an end-to-end process built on over 15 years of experience, focused on keeping customers safe on Google applications like Gmail, Search and other Apps.

Google Cloud platform and infrastructure are certified for a growing number of compliance standards and controls and undergo several independent third-party audits to test for data safety, privacy, and security.

ToogleBox has passed all the security and usability requirements of the G Suite Marketplace and can be installed only from there.

OAuth 2.0

ToogleBox users have access to their G Suite domain through the OAuth 2.0 open standard. This means that they never expose their G Suite account credentials.

Single Sign-On

ToogleBox doesn't ask for any user passwords and doesn't alter or keep them. User authentication and consent are handled by Google.

User authentication is done by receiving from Google authorization codes to be exchanged for access/refresh tokens. Access tokens are used by **ToogleBox** to access Google APIs.

Secure Browser Connections

As a service based on and devoted to Google, **ToogleBox** uses Google Appspot secure HTTPS connections.

All HTTP, non-secure requests are automatically redirected to the corresponding HTTPS URL.

The connection is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (ECDHE_RSA with X25519), and a strong cipher (AES_128_GCM).

G Suite Data access

ToogleBox uses the following Google APIs and SDKs to interact with G Suite. All APIs use authorizing requests with OAuth 2.0:

- G Suite Marketplace API and SDK
- Contacts API
- Admin SDK (User, Domain list, Group, Customer)
- Gmail API (Email, Signature)
- Google Plus API

Storage

ToogleBox information resides in Google's data centers. It uses Google Cloud SQL for persistent data. Some BLObs and images are stored in Google Cloud Storage. Transient data is kept in the Google Datastore.

Storage control access and visibility to resources are protected by Google's Security Model.

Cloud SQL security

ToogleBox uses Google Cloud SQL, which provides a 99.95% availability, swift scalability, automated backups, replication, patches, and updates.

Cloud SQL data is encrypted when on Google's internal networks and when stored in database tables, temporary files, and backups.

Every Cloud SQL instance has a network firewall that controls network access.

Access to each database instance is granted to named user accounts whose password is changed monthly.

Access is done through SSL Connections and is restricted to a small set of controlled IP addresses.

SSL certificates are renewed semi-yearly.

System Development

ToogleBox functionalities are subject to constant change. Change is promoted by three factors:

- Requirements from the user base which result in specs for improvements.
- Technical changes and new functionalities in G Suite require changes and inspire the development of new features.
- New threats posed to G Suite users by hackers and other wrongdoing actors.
- New features.

Change Control

ToogleBox developers use the Extreme Programming (XP) methodology for maintenance purposes. In order to mitigate a negative impact on security, performance or function, all changes, bug fixes, and improvements go through the following tests:

1. Unit test in Dev environment
2. Integrated test in Beta environment
3. Functional assessment in Beta environment
4. Security scan in Beta environment
5. Smoke test in Prod environment

Development is made in a controlled environment. All developers require privileges, user Id and passwords granted under the Google Security Model.

Security scans

ToogleBox is periodically checked with three types of penetration test performed by two separate companies:

1. Veracode static scan: Veracode Static Analysis is a Static Application Security Testing (SAST) solution that enables the identification and remediation of application security findings. The Veracode static scan runs once per month and whenever major changes take place.
2. Veracode Dynamic Analysis scan: Veracode Dynamic Analysis is a Dynamic Application Security Testing (DAST) solution that delivers an automated and scalable dynamic scanning capability that enables broad coverage at speed. The Veracode dynamic scan also runs once per month and whenever major changes take place.
3. Manual Penetration Test by CySec Solutions: CySec Solutions runs a semiannual penetration test.

ToogleBox Development Team uses Veracode SourceClear, a Software Composition Analysis (SCA) solution.

Functional Security Features

ToogleBox is a powerful damage control tool that performs sensitive actions. Its use is thoroughly recorded and informed to Superadmins and other designated users.

Restricted user access

Only Superadmins can install **ToogleBox** from the G Suite Marketplace. Initially, they are the only authorized users of **ToogleBox**.

At all times, only Superadmins have access to the Configuration Panel and their privileges are repeatedly validated through API Permission Check. Hence, users deprived of Superadmin privileges will automatically lose access to the Configuration Panel.

Superadmins can grant access for regular users to utilize **ToogleBox** services, but their Superadmin privileges cannot be granted.

Logging

ToogleBox keeps a fully-detailed log of all processes, user-performed tasks, and even user navigation within the GUI.

History

ToogleBox keeps security data for each task:

- Service performed
- User identification
- IP address
- Timestamp
- Parameters used

This data is emailed in real time to Superadmins and other designated users. Task History has a 5 year retention period and is easily retrievable from the GUI.