Torii Extension Design White Paper

Last updated: January 2022
Extension version: 1.0.163 and above

Introduction

Torii is a SaaS management tool which gives IT the ability to discover, optimize and control their organization's SaaS usage and costs.

Torii utilizes several ways to discover SaaS applications, the browser extension is one of them (more info on how Torii works can be found here - https://toriihq.com/product)

We pay high attention to our users' privacy and our goal is to be transparent on how Torii gathers information, therefore many security and privacy aspects were taken into account when designing the browser extension. This document gives as much information as possible on how Torii browser extension works behind the scenes.

https://www.toriihq.com

Principles

The following principles guides us when designing the extension:

1. **Privacy by Design**
   Do not collect any sensitive data related to users.
2. **Reduce Collected Data**
   Collect as little metadata as required to provide the tools to the administrator.
3. **Transparency**
   Document and make the extension functionality clear to both administrators and users.

Extension Overview

Torii automatically produces application and user usage reports to help your company make better SaaS decision.

The extension analyzes user behavior to detect logins to business applications. **The entire analysis is being performed locally on the client side**, meaning that no cookies nor login information is being sent to Torii servers. Once a SaaS application is detected the only information recorded is the Torii user ID, application name and the time stamp of the visit.

The extension is consists of three main components:

1. **UI Component**
   The UI shown when a user clicks on the extension's icon.
2. **Content Script**
   A on-page script that detects the user's email and if he is logged in to the current service.
3. **Background Logic**
   This is the logic of app detection and the only component communicating with our servers. It also communicates with the UI and Content-Script components.

The extension only maps business SaaS applications and does not analyze or store personal usage. It only operates on a hand-picked list of SaaS business applications ("*Application Whitelist*").

- **Examples of apps that are mapped:**
  SalesForce, HubSpot, New Relic, MailChimp, and any app that is used for business purposes.
- **Examples of apps that are not mapped:**
  Facebook, LinkedIn, Twitter and any other personal apps.
- **Mixed usage:**
  Some applications may present versions for personal and versions for business use, such as Facebook vs Facebook ads, LinkedIn vs LinkedIn Recruiter, Twitter vs Twitter ads. Torii only maps their business usage

For additional information and FAQ, see: https://toriihq.com/extension

Permissions

The extension only requires the minimum set of permissions required to perform its app detection tasks. These are the required permissions:

- **`identity`** and **`identity.email`**
  Used to identify the email of the currently signed in user to the browser.
- **`cookies`**
  Used to identify the email of the user by looking at stored emails in cookies. Also used to acquire the CSRF token for the *toriihq.com* domain in order to protect the privacy of Torii users.
- **`history`**[1]
  Used to read website visits of specific domains in order to detect usage of SaaS.
- **`tabs`**
  Used to opening new browser tabs from the extension's UI and reading the tab's URL information.
- **`storage`**
  Used for storing local cache for user identity, detected apps and recent activity.
- **`<all_urls>`**
  Used for access to metadata information for visited URLs. The extension limits itself to a pre-defined list of SaaS related domains.

The full documentation for all permissions can be found on:
- Chrome: https://developer.chrome.com/apps/declare_permissions
- Firefox: https://developer.mozilla.org/en-US/Add-ons/WebExtensions/manifest.json/permissions

[1] Chrome history API gives both read and modify access to the browsing history. There is no read-only history API at the moment. Torii does not modify user browser data and only uses read access.

How Data is Secured

We build our systems to reduce the amount of data needed to be collected and transmitted over the network. All data that can be processed on the end-user's browser will not be send to any server.

All metadata that is being transmitted, is encrypted both in transit and at rest. Database instances, including read replicas and backups are encrypted using the industry standard AES-256 encryption algorithm. Encryption is enforced via TLS to all data in transit. The databases are hosted on Amazon RDS in the US regions using a Multi-AZ deployment for enhanced availability and durability.

Only secure (HTTPS) access to Torii's servers are allowed. Non-secure HTTP request are first redirected for the HTTPS endpoint before they can be served.

How Users are Identified

The Torii browser extension can operate in two modes: **Authenticated** and **Unauthenticated**. This can be configured from the settings page in your Torii dashboard. In **Authenticated mode**, end users are required to login and are identified only by a successful login.

In **Unauthenticated mode**, the extension does not require its users to login. There is a procedure to identify the user's email as detailed below.

1. The browser is queried for the email address of the signed in user.
    - If email matches the organization's email domain, this email will be taken and there is no need for further steps.
    - Otherwise, if email is not available or does not match organization's domain, move to the next step.
2. The extension searches for email address in all of the stored cookies.
    - If the same email is found more than 3 times, this email will be taken and there is no need for further steps.
    - Otherwise, if email is not available or does not match organization's domain, move to the next step.
3. The extension identifies the email address by monitoring logins to SaaS applications. Whenever an email with the organization's domain is used for login, it will get 1 point. When the threshold of 2 points is reached, meaning a user logged-in to two different SaaS applications with the same email, this email will be taken.

The identification process can be immediate if options 1 or 2 are used, or take up to 48 hours (on average) when option 3 is used.

How SaaS Applications are Detected

Once identity was detected, the SaaS app detection process starts. The extension will only detect SaaS applications where the identified user is registered to, rather than just visiting their marketing pages.

Torii uses a variety of methods to detect the usage of applications:

1. **Detection by login attempt**
   When a login form is detected, by the presence of an `<input type="password" />` on the page, the extension will look for `<input />` with the value of the detected app. This is a signal that the user has an account in this SaaS application.
2. **Detection by "email on page"**
   When a page's DOM has the identified user's email on the DOM this is a signal that the user has an account in this SaaS application.
3. **Detection by "keywords on page"**
   When certain keywords are on a page (such as "Log out", "Sign out", etc…) is present on the DOM, this is a signal that the user has an account in this SaaS application. To verify that this app is used in business context, the extension also searches for presence of the company's name on the page.

How SaaS Applications Usage Data is Reported

Each visit to a website whose domain appears on the "Application Whitelist", will be logged and reported. This is done by logging the time and domain that were visited. No other data is logged.

Example:
User navigates to https://www.example.com/information/contact_details
The extension logs the time and domain `www.example.com`, but will **not** log the `/information/contact_details` path.

Conclusion

The Torii team is dedicated to protecting the privacy of its users and providing full transparency in the design of our software. Please contact support@toriihq.com for further questions.

Torii
https://www.toriihq.com