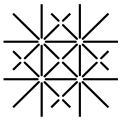

University of Basel

# Sandbox Implementation for Enterprise Collaboration Platforms

Scientific Writing Seminar Final Paper

Natural Science Faculty of the University of Basel
Department of Mathematics and Computer Sciences

Examiner: Prof. Dr. Craig Hamilton
Supervisor: Dr. Tanja Schindler

Tri Nguyen
tri.nguyen@unibas.ch
24-065-948

20th December 2024

# Abstract

Collaboration Platforms, such as Monday.com and ClickUp, have revolutionized enterprise workflow management, generating billions in revenue by integrating multiple functionalities into a unified platform. However, as organizations integrate more third-party apps, security concerns arise—particularly around data privacy, access control, and system integrity.

We present a sandbox solution with enhanced functionality while maintaining robust security. Our evaluation shows that the sandbox enables granular access control, broadens the technical capabilities of third-party apps and enhances the developer experience.

# Table of Contents

# 1

# Introduction

One of the most pervasive challenges faced by organizations is the existence of data silos—disconnected, fragmented pockets of information that reside in isolated platforms or applications. Data silos present significant challenges for knowledge workers, who often find themselves navigating a maze of isolated data sets, each requiring manual coordination between teams.

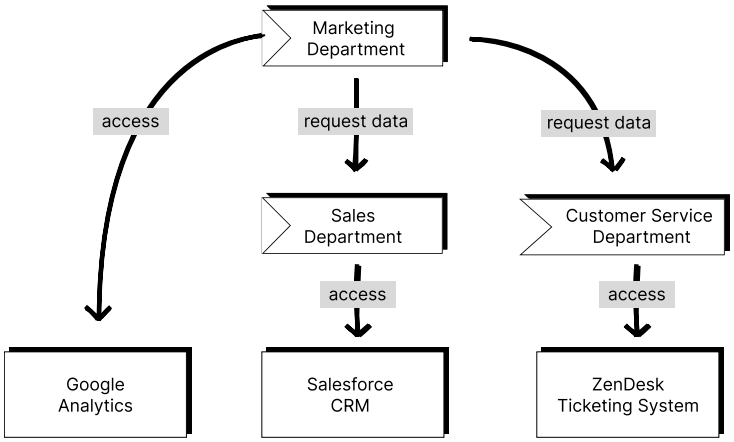


Figure 1: The Marketing Department struggles to combine three different data sources for a new advertising campaign.

To illustrate the impact of data silos, consider a typical scenario within an organization. The Marketing Department may want to launch a new advertising campaign but only has access to Google Analytics, a tool that provides user behavior data. To obtain a broader understanding of customer profiles and the issues customers are facing, they must contact the Sales and Customer Service departments—each of which stores its data on different platforms. The result is a cumbersome process of collecting and consolidating data from three different sources—a process fraught with delays and coordination challenges.

This has led to many organizations turning to *collaboration platforms* as a lightweight and user-friendly approach to solving the data silos problem.

## 1.1 Background

Collaboration platforms bring together a suite of tools—such as messaging apps, project management tools, wikis, meeting schedulers, and CRMs—into a unified space. This integration makes it easier for teams to share and access the data they need without navigating multiple systems or encountering fragmentation.

Many collaboration platforms, in order to cover a wide range of business use cases, invite third-party developers to build and integrate their applications into the platform. However, due to the difficulty of implementing a properly secure sandbox system, these platforms often resort to restricting third-party app functionalities instead. As a result, these apps typically store core logic and data outside the platform, have limited control over the platform's user interface (UI), and require developers to learn niche, platform-specific frameworks.

Thus, these apps neither extend the platform's functionalities in a meaningful way nor are they easy to develop.

| Platform | Third-Party Data Integration Capability | UI Customization | Platform-agnostic Development Framework |
|---|---|---|---|
| Lark | Low | Limited (pre-made blocks) | No |
| ClickUp | Moderate | No customization | Yes (via API calls) |
| Monday.com | Moderate | Limited (pre-made blocks) | Yes (via API calls) |
| Asana | High (via Work Graph®) | Limited (pre-made blocks) | No |
| Salesforce | High (via Standard Objects) | Full customization | No |

Table 1: Overview of third-party app support across collaboration platforms.

## 1.2 Objectives

The primary objective of this work is to develop a secure, browser-based sandbox solution that addresses the challenges of integrating third-party apps within collaboration platforms. The lack of existing solutions creates a significant barrier for platform developers seeking secure and flexible third-party app integration.

The sandbox model aims to achieve several key goals:

- **Protection of critical resources**: Any potentially harmful code is confined within a controlled environment, preventing third-party apps from executing unauthorized actions. Essential platform resources are protected from third-party code, ensuring system integrity.

- **Ease of third-party app development**: Supports universial frameworks like React, Angular, or Vue with development features like Hot Module Reload (HMR). The model is designed with data access and UI customization capabilities in mind.

- **Performance**: The sandbox does not degrade the platform and remains close to the performance of native, unsandboxed code.

# 2

# Related Works

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae.

- Iframe, Web worker and Service worker
- WebAssembly
- SES
- Salesforce Ligning Framework
- Sandstorm.org
- Webcomponents

# 3

# Implementation

## 3.1 Model Overview

Each sandbox is an isolated environment that limits third-party apps to a controlled subset of sensitive resources. These resources are owned by the browser (e.g., the DOM, web APIs like camera, cookies, and network), the business (e.g., proprietary data), or the platform itself. Access to these resources is governed by the sandbox's permissions, which are granted by the platform, IT administrators, or end users. Resource usage is transparent to the platform, which can introspect or revoke access at any time.

A platform can run multiple sandboxes simultaneously, each with its own set of resources and policies. This model is particularly well-suited for collaboration platforms, where each instance of a third-party app operates within its own sandbox.

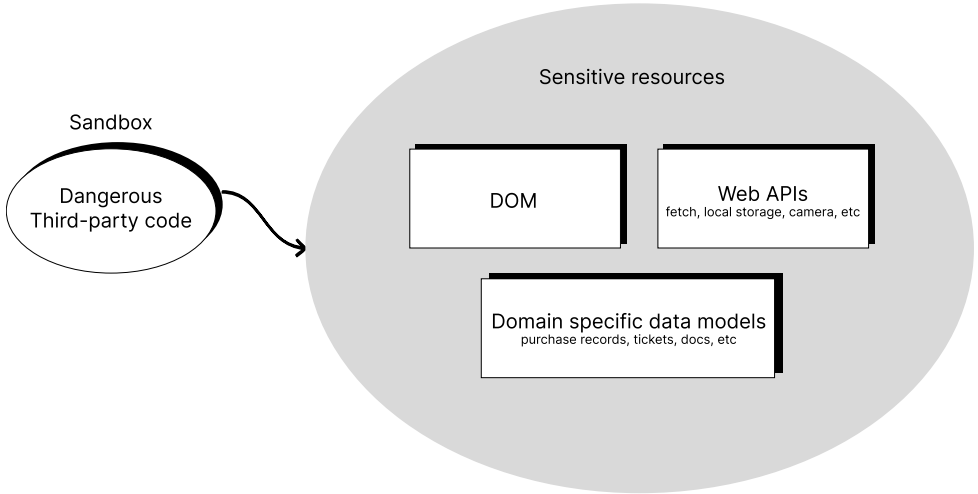


Figure 2: Isolating third-party apps within a sandbox, with controlled access to platform resources.

The sandbox also distorts the functionality of several web APIs to enhance security and improve the development experience through isomorphism. For example, the following JavaScript code snippet appears similar to that of a normal web app, but behaves differently within the sandbox:

```
// fetch is distorted to automatically checks the domain against a whitelist
const response = await fetch('https://example.com/api/reservations')
const data = await response.json()
// localStorage.setItem is distorted to prevent storing the data
// forwarding it instead to a separate data store
// Each app then has a non-conflicting, isolated data store
localStorage.setItem('data', JSON.stringify(data))
// getElementById is distorted to query only elements
// under a specific DOM node granted to the sandbox
const element = document.getElementById('app')
// element.innerHTML is distorted to sanitize the HTML before setting
element.innerHTML = JSON.stringify(data)
```

The list of distortions is not exhaustive and will be expanded as new web APIs emerge. Since automatically introducing an undistorted API could pose a security risk, each version of the sandbox maintains a list of supported APIs and only exposes those to the third-party app.

## 3.2 Technolgies Used

Under the hood, the sandbox treats each app as a collection of HTML, CSS, and JavaScript files, each with its own security requirements. Several different technologies are combined to achieve the desired sandboxing functionality.

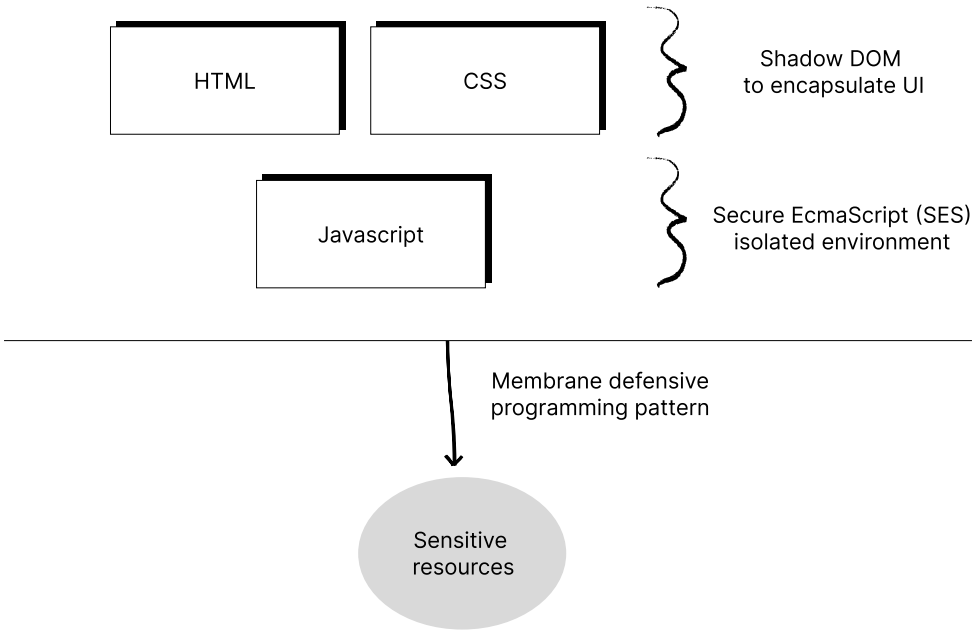


Figure 3: Technologies corresponding to each part of the sandbox model.

### 3.2.1 For HTML and CSS

For HTML and CSS, Shadow DOM is used to prevent style leakage from the app to the platform. Shadow DOM is a browser-native feature that allows the creation of an isolated UI environment for each app, as also used by Web Components. Each sandbox has access to a shadow root node that it fully controls. Necessary distortions are implemented to stop querying elements outside the shadow root (e.g., via `shadowRoot.ownerDocument`).

### 3.2.2 For JavaScript

For JavaScript, the sandbox uses the Secure ECMAScript (SES) library by EndoJS to lock down global prototypes (preventing prototype pollution attacks) and create a compartment where access to web APIs is disabled by default and can only be enabled via endowments. Unlike iframes or Web Workers, SES does not require a separate thread to run the code. Instead, the code runs in the same main thread as the platform, making it more efficient and avoiding communication overhead while allowing shared object address space.

### 3.2.3 For Resource Access

To enable granting and revoking access to resources, as well as applying distortions, the sandbox uses the Membrane defensive programming pattern. First introduced in the Caja compiler paper, the Membrane pattern is simpler than other capability-based security measures, automatically covers all web APIs via deep annotation, and remains theoretically secure. When implemented in JavaScript, the pattern leverages ES6 proxies: by exposing only the proxy instead of the underlying resource object, the sandbox can distort certain operations on the object through the proxy's handler. Any object returned as a result of these operations is also wrapped in a proxy.

## 3.3 Developer Experience

We aim to deliver a developer experience that closely resembles a typical web app. To this end, the sandbox takes further steps to ensure a seamless workflow:

- Instead of requiring a manifest file to define which entry points to load, the index HTML file is parsed to find entry points. This means external files are fetched, while inline CSS and JS are sanitized and evaluated.

- Dynamic imports and ES modules are supported, as they are the primary mechanism for development servers (e.g., Vite) to load and replace code (e.g., hot module replacement, or HMR). Since JavaScript dynamic imports are part of the JavaScript specification (not a web API), this is implemented by analyzing the source code and replacing the import statement with a function call. This function fetches the file and returns an ES module object.

As a result, the developer experience is virtually identical to that of a normal web app while maintaining the benefits of sandboxing. The developer can use the same tools and frameworks as they would for a normal web app. They can open a localhost development port and let the platform to connect and load the app.

# 4

# Evaluation

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae.

## 4.1 Performance Metrics

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae

non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae.

## 4.2 Security Assessment

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et.

# 5

# Discussion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae.

# B

# Bibliography

Shown [1] and [2]

[1] G. Prekas, M. Kogias, and E. Bugnion, "ZygOS: Achieving Low Tail Latency for Microsecond-Scale Networked Tasks," in *Proceedings of the 26th Symposium on Operating Systems Principles*, Association for Computing Machinery, 2017, pp. 325–341. doi: 10.1145/3132747.3132780.

[2] J. Mehta and E. Kinnear, "Boost Performance and Security with Modern Networking," Jun. 26, 2020. Accessed: Sep. 17, 2020. [Online]. Available: https://developer.apple.com/videos/play/wwdc2020/10111/