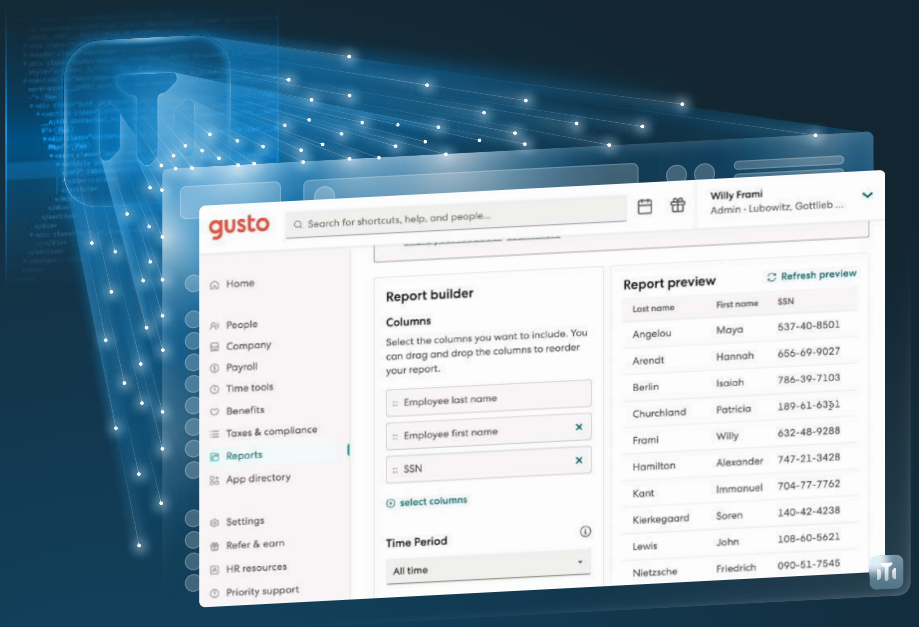
MirrorTab

Protect Your Customers Against Client-side Attacks

Your trust and reputation depends on it.

G/ A GOOGLE VENTURES COMPANY

HT INTRODUCING HOLOGRAM TECHNOLOGY



Client-side Isolation

We create a virtual air gap between web apps and end-users accessing them to enhance security.

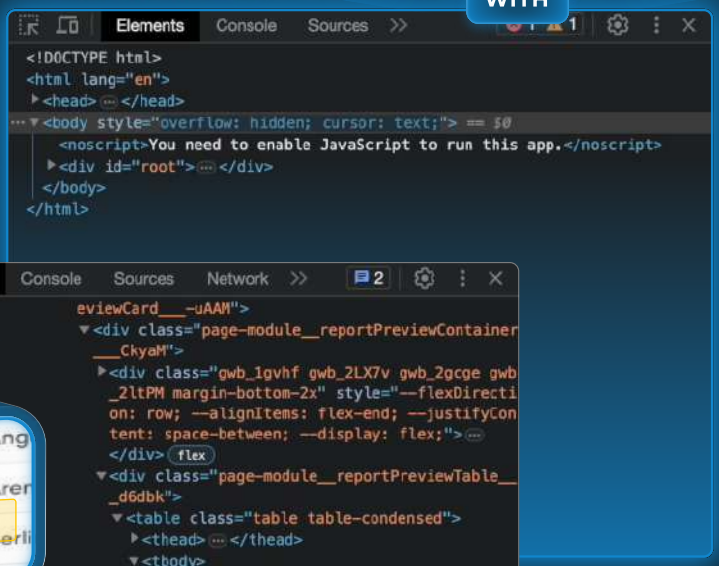
Pixel Streaming

We stream pixels instead of Document Object Model (DOM) elements, removing the attack surface against threats.

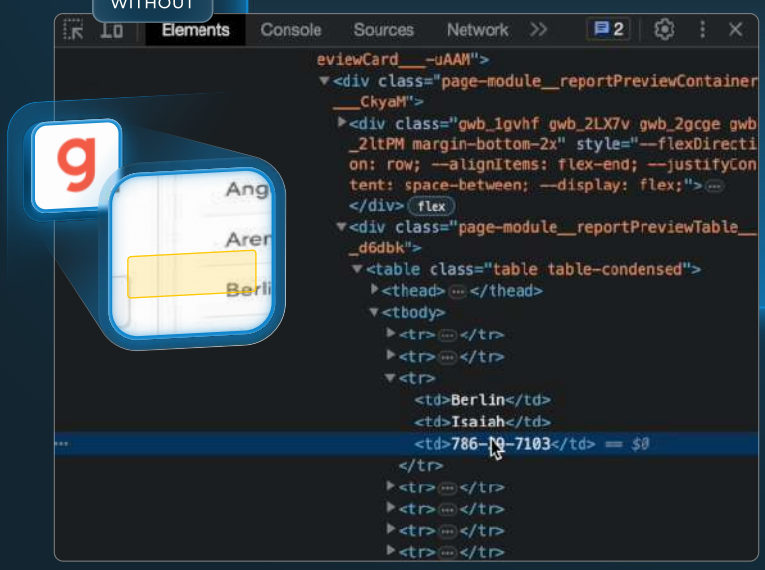
Deployed Server-side

We maintain a frictionless user experience, with no client-side behavior changes or web app modifications required.

WITH



WITHOUT



* We are showcasing Gusto as our example web app based on their online demo. MirrorTab works similarly with all web applications.

A proactive defense to protect your web apps, improve client-side security, and enhance customer trust.

MirrorTab's hologram technology streams secure virtual representations of web applications, isolating customer interactions, obfuscating data and APIs from client-side security threats.

Instantly secure customers against:

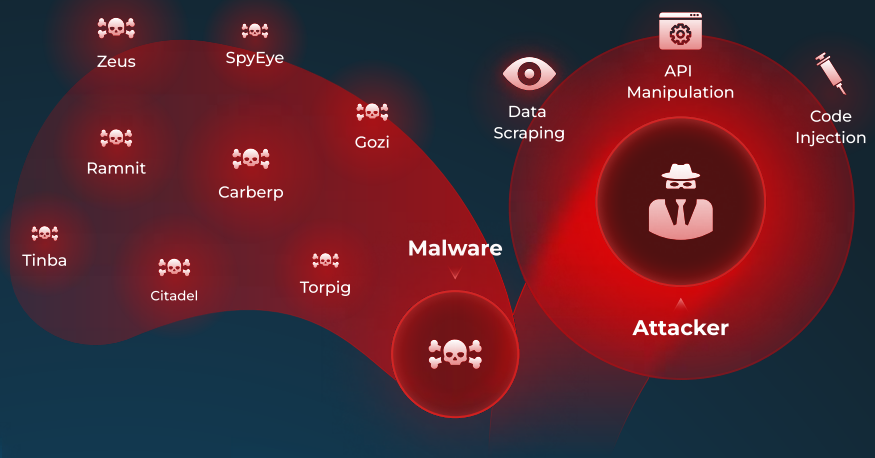
- DOM XSS
- Open redirection
- Cookie manipulation
- JavaScript injection
- WebSocket-URL poisoning
- Link manipulation
- Web message manipulation
- Ajax request-header manipulation
- Client-side SQL injection
- HTML5-storage manipulation
- Client-side XPath injection
- Client-side JSON injection
- DOM-data manipulation

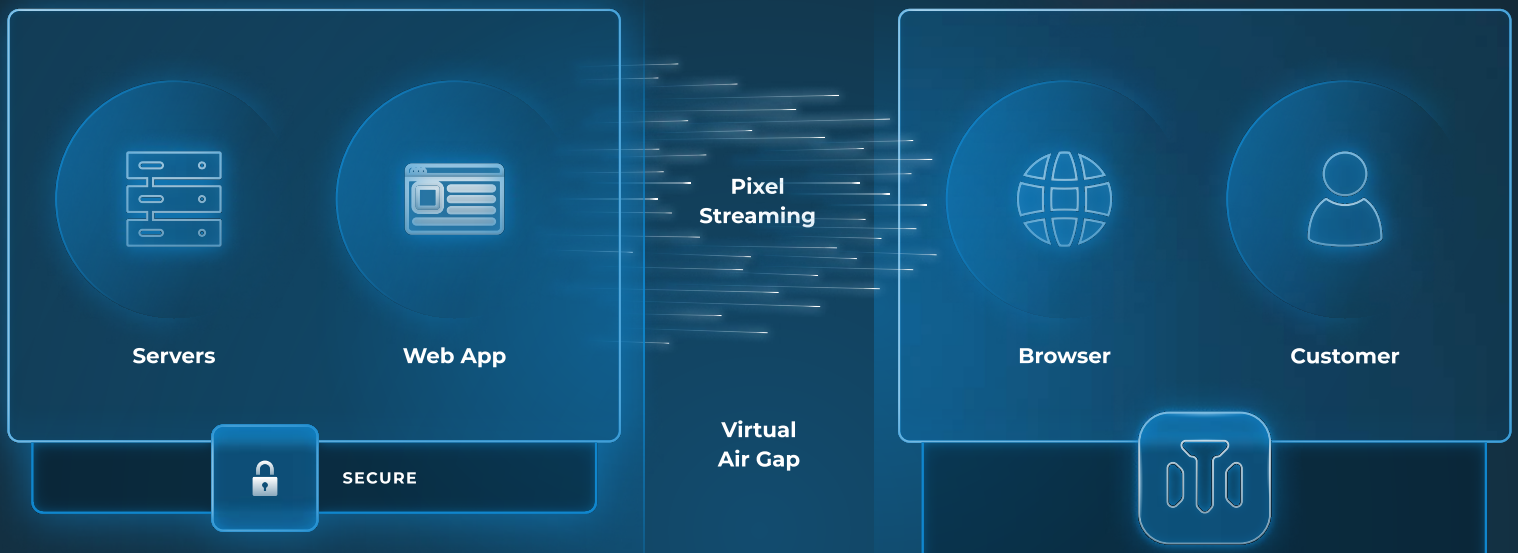
Look at back for more details on client-side protection capabilities. →

Protect Customer Interactions and Web Apps from Client-side Attacks

By removing access to the DOM we prevent data scraping, API manipulation and remove the attack surface for malware injection.

We effortlessly secure customer interactions and web apps, preserving trust in your software and services.





Stop Data Scraping

Keep your customer's data secure.
No elements for DOM-based data scraping.

Data is clearly visible in the DOM as plain text and code as it gets processed in the browser, and can be easily accessed and stolen from client-side attacks by bad actors.

Prevent API Manipulation

Keep bad guys from getting under the hood.
No visible API calls to be manipulated.

API calls, credentials, session tokens, and network activity are clearly visible in the DOM, and if they are not properly engineered, protected, or maintained, bad actors will take advantage.

Thwart Code Injection

Keep customers secure even if web sessions are infected.
No attack surface for malware.

Malicious actors use client-side code injection to interact with DOM elements, residing as a browser extension or a trojan to orchestrate malicious activity on the user's behalf.

We protect against:

- Cross-site Scripting (XSS)
- DOM-based XSS
- Directory Traversal or Path Traversal
- E-skimming
- E-commerce Platform Skimming
- Drive-by Web Skimming
- Trusted Cloud-hosted Platform Skimming
- Anti-forensic, Self-cleaning, and Stealth Data Skimming
- Credential stuffing
- JavaScript Injection
- SQL Injection
- XML Entity Injection
- Formjacking
- Sideloading & Chainloading
- JavaScript Sniffing
- Broken Link Hijacking
- Server-side Request Forgery
- Cross-site Request Forgery

And many more...

Founded by founders of Honey (acquired by PayPal).

Built by an all-star team of engineers from:

To learn more visit: **mirrortab.com**