Introducing
The Enterprise Browser:

Delivering control, visibility, and governance over data and applications via the browser.

WHITE PAPER
FEBRUARY 2022

Island

Executive Summary

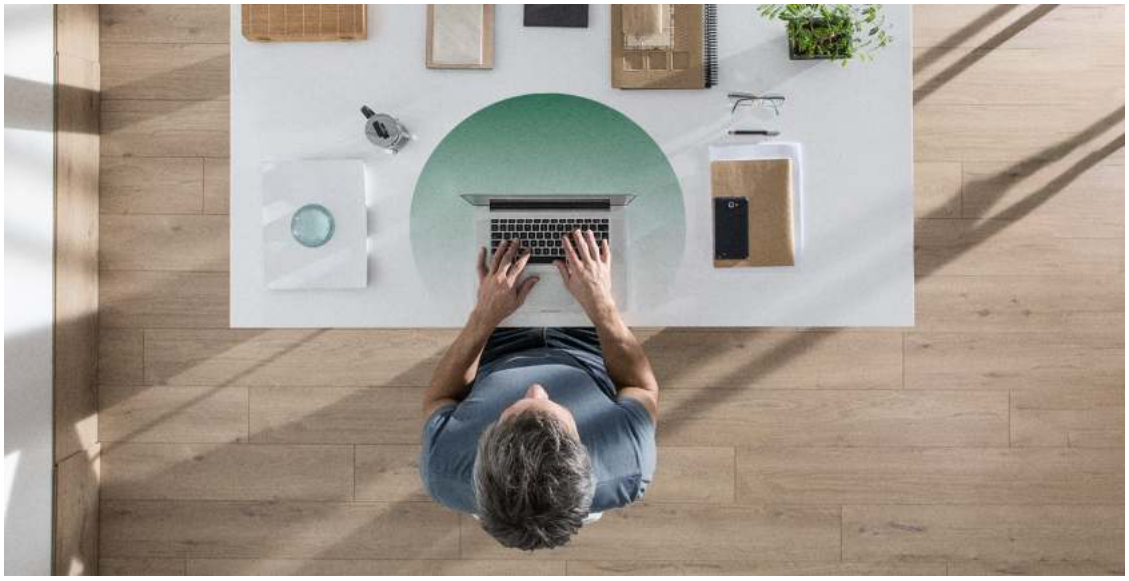
The browser has become the most commonly used application in the enterprise.

The consumer browser was never designed to be an enterprise application, causing organizations to overcompensate with a complex and expensive security stack that is increasingly unreasonable to manage and incredibly frustrating to work with for users and security teams alike. Island is the world's first Enterprise Browser that naturally embeds the core needs of the enterprise into the smooth, familiar, Chromium-based browser experience.

Now, organizations have complete control over the last mile, with the ability to govern and audit all browser behavior, customize the browser to support its unique identity, workflows, and needs, and feed all browser data to the rest of the enterprise, radically improving the effectiveness of their entire infrastructure. This approach can fill in the missing puzzle pieces of a zero-trust initiative ensuring a natural fit for an evolving workforce and web-based applications that can live anywhere. Securing work more effectively without compromising on the smooth, enjoyable browser experience users expect.

With The Enterprise Browser, security extends everywhere it's needed without getting in the way of work. Which means SaaS and internal web apps no longer leak data to the end point, BYOD and contract workers just log in and get to work without putting data at risk, user privileges are now safe from misconfiguration or tampering, consumer or risky applications are now safely permitted inside the workplace, and much more.

It's work as it should be - fluid, frictionless, and fundamentally secure.



Introduction

Consider the following question: Which applications do enterprises use most?

Despite such universal adoption by enterprises everywhere, the browser isn't even an enterprise application. It was built to serve consumers, advertisers, and content providers.

You might be thinking Microsoft Office. Maybe Salesforce. These are quite frequently used. But there's another that's used far more often by the greatest number of enterprises, and that is the browser. In the age of anywhere, the browser is where all our employees, apps, and data meet. And it's where virtually all our work happens.

Yet, despite such universal adoption by enterprises everywhere, the browser isn't even an enterprise application. It was built to serve consumers, advertisers, and content providers. Designed to track user data, deliver hyper-targeted ads, and accelerate content search and discovery. Optimized for the best possible user experience - fast rendering, powerful extensibility, and universal compatibility. And because it has served the user so well, we brought the consumer browser to work as well.

But since the browser was never intended for the enterprise, it lacks the core elements any enterprise needs to work safely and productively. Basic governance, visibility and security - they're simply not there. Our security teams are essentially locked out of the one application our organization depends on most.

Because the browser doesn't cooperate with the enterprise, we're given no choice but to surround it with gateways, CASBs, DLP solutions, firewalls - an endless array of security solutions. And in the process, our stack becomes too complex, expensive, and fragile to maintain. We're forced to make painful tradeoffs that leave our organization too exposed or work too confined.

And we're still blind to what's actually happening in the browser - unprepared to protect the critical resources our organizations hold dear. And ironically, the reason we chose the browser in the first place - it's smooth end user experience and simple manageability - is replaced by frustration, disruption, and delays to work itself. Pain shared by both users and security teams alike.

It's not the browser's fault. It was never designed to serve the enterprise.

Well, what if it was?

Imagine if instead of the enterprise having to operate on the browser, the browser was fully integrated into the enterprise. Imagine if all the core elements your organization needed to work securely, were built into the same browser experience you're using right now.

Introducing Island. The Enterprise Browser.

So often, enforcing new security tools like sandboxes, agents, or virtual desktops comes at the cost of a convenient end-user experience.

The Enterprise Browser is the ideal enterprise workplace where work is fluid while remaining fundamentally secure.

With the core needs of the enterprise naturally embedded in the browser itself, Island gives organizations complete control, visibility, and governance over the one place where nearly all their work happens, while delivering the same smooth Chromium-based browser experience users expect.

And with a browser that actually cooperates with the enterprise, everything around it gets smarter, simpler, and easier. Files are now scanned by data-loss prevention, malware, and other security tools before being downloaded, uploaded, or viewed. Browser activity is fed directly into your SIEM or other analytics platforms, completely avoiding the complexities of decrypting and inspecting SSL traffic in the network to perform these actions. And because it's a browser, encrypted traffic is natively terminated to deliver a natural experience with complete visibility.

Island can sit alongside your existing browser for individual critical applications and activities that require maximum control, governance, or visibility. Or it can serve as your primary browser for all work activity. And with the Enterprise Browser, work is suddenly much simpler yet completely secure at the same time, across a wide range of enterprise scenarios such as BYOD, contractor access, new web applications, privileged user needs, legacy application access, and more.

The Foundation: Chromium

The element that made the browser such an attractive work application in the first place was its user experience. Its smooth, fast rendering, an ecosystem of extensions , and universal compatibility are just some of the reasons why it's been the most widely adopted application on earth. But when it comes to security solutions, adoption becomes a serious challenge. So often, enforcing new security tools like sandboxes, agents, or virtual desktops comes at the cost of a convenient end-user experience. And in more than a few cases, users are unwilling to embrace those solutions for day-to-day work.

By controlling what the browser presents to end users, Island becomes the most powerful ally in ensuring sensitive data is only seen by the right users and used in the right way.

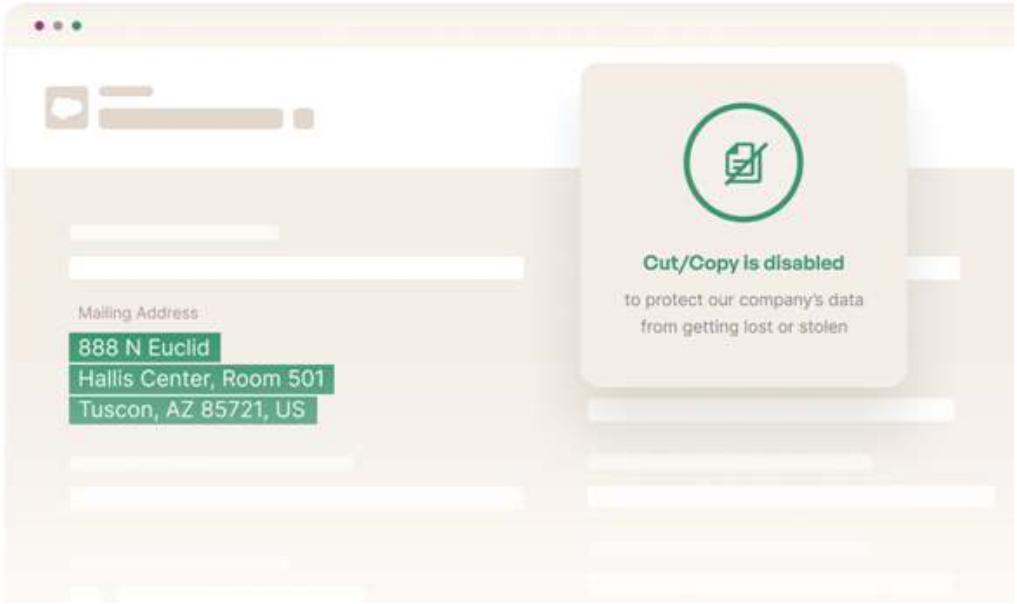
We understood that, for the Enterprise Browser to be implemented and actually adopted, it cannot come at the price of the experience. That's why we built The Enterprise Browser using the open-source Chromium project - the same technology that powers the most widely adopted consumer browsers like Google Chrome and Microsoft Edge. Chromium delivers the core services of user experience, rendering, JavaScript interpretation, codecs, extensions, and networking for that stable, familiar experience users expect. Which means users will have an experience identical to the browser they use today — completely removing the struggle of adopting a new security security solution for day to day work.

Securing the Last Mile

At the heart of any enterprise application is the means to granularly control, govern, and secure the work being done on it and the data it contains. Yet, when it comes to consumer browsers, the moment our data reaches the window of the browser itself, it is essentially ungoverned by any of the traditional controls we depend on to secure our critical information.

Despite our efforts to secure the applications themselves and the networks they travel on, it's this "last mile" - the browser window itself - where protection is out of the enterprise's hands. Once data arrives there, users can do what they please, creating a nightmare for the enterprise. This leaves organizations at the mercy of their user population, praying they use corporate web applications and their underlying data properly. Yet, this uncomfortable reality raises all sorts of difficult questions for security teams, such as:

- What's stopping a user from copying and pasting sensitive data onto a personal application?
- What's stopping a user from printing, screen capturing, or taking a photo of critical information on their screen?
- How do we give access to a corporate application while preventing that same user from seeing sensitive data on that same app?



- How do we stop one kind of user from downloading or uploading data to or from critical apps without it impacting other users?
- How do we empower the use of personal devices while at the same time protecting critical resources?
- How do we ensure a safe experience even when users aren't on a managed network or VPN?

But with Island, enterprises can take ownership of the entire browser experience like never before.

Until now, those protecting the organization were forced to either turn a blind eye to these questions or accept answers they weren't comfortable with. The inconvenient reality is, without seeing or controlling what's happening in the browser, there's very little that can be done.

All of this changes with The Enterprise Browser. With The Enterprise Browser, you have complete control over this last mile. Security teams can set deep, granular policies that govern how the browser behaves across every user, in every scenario, from the universal level down to the finest details of an application.

By controlling what the browser presents to end users, Island becomes the most powerful ally in ensuring sensitive data is only seen by the right users and used in the right way.

For example, using Island's management console, you can set a policy allowing users to access only certain areas of a specific application depending on their role, device posture, network connection, and other parameters. And through this policy, you can control all types of interactions with the contents of the screen, such as:

- Copy/pasting within or between applications
- Screen captures of an application
- Printing application pages
- Saving screen content
- File download or upload within an application
- Adding multi-factor authentication to certain areas of an application
- Masking sensitive on-screen data without any backend database changes
- Watermarking to prevent phone or camera screen capture

These are just some of the countless examples of how the Island Enterprise Browser keeps the data inside critical application resources comprehensively secure in ways that simply weren't possible until now.

Auditing and Logging Browser Activity

The typical enterprise today has a whole toolbox of solutions dedicated to monitoring and logging user behavior and auditing possible problematic events - tools such as web proxies, endpoint controls, data loss prevention technologies, identity providers, and cloud access security brokers, to name a few. But as long as work is done on a consumer browser, the best these tools can search for are clues.

With no visibility into how users behave inside the browser, organizations are limited to gathering bits and pieces of information found beyond the browser, but never fully seeing the activity itself. This is quite simply due to the fact that the consumer browser was never designed with enterprise visibility in mind, and as such, does not cooperate with enterprise visibility tools in any meaningful way.

Now imagine what those tools can do if they were integrated into the browser instead of locked out of it. The Enterprise Browser gives you the ability to capture and log any interaction so you can monitor or investigate incidents in amazing detail. You can even have Island capture a screenshot of any given activity to have visual proof of more critical interactions.

And in addition to viewing all browser activity inside Island's management console, Island can also feed browser activity data into your existing SIEM or other analytics tools, giving your entire infrastructure a level of visibility that was simply not possible before.

Security teams now benefit from seeing the complete picture of all user activity and experience, and take more direct, more impactful action to keep the organization secure as a result.

Island can also feed browser activity data into your existing SIEM or other analytics tools, giving your entire infrastructure a level of visibility that was simply not possible before.

Making the Browser Yours

With the consumer browser being the default environment for work until now, the option to customize the browsing experience to match our organization's unique identity, workflows, or corporate needs was never a consideration.

But with Island, enterprises can take ownership of the entire browser experience like never before. Customize the brand color, look and feel, even its tone of voice to match your unique organizational identity. Insert company-specific workflows. Add custom browser-based robotic process automation (RPA) scripts that trigger over an application within the presentation layer of the browser to serve your unique needs, without requiring any changes to the actual application whatsoever.

For example, most financial institutions enforce multi-factor authentication to verify logins. But today, this is only done at the initial login, allowing users to view data or execute sensitive actions without any further limits or verifications. But in the Enterprise Browser, you can automatically insert MFA to your identity provider before executing a wire transfer or other sensitive actions.

This is just one example of the countless ways you can extend the Enterprise Browser into the single most powerful method for securing your data across the organization.

By introducing Browser-based RPA into the browser, Island enables you to customize your enterprise work experience with automations, company-defined workflows, and cross-application integrations - all executed from inside the browser, over any SaaS or internal web application, without needing to touch the application itself.

Enhancing Your Entire Infrastructure

For decades, we've had to operate our security stack without any cooperation whatsoever from the browser. In a sense, we've had to treat the browser like a 'caged animal'. Because of our fundamental inability to secure the browser from within, we've asked our surrounding security tools to overcompensate by working harder than necessary to keep our organization safe.

Data Loss Protection solutions had to seal every exit from the browser - even the ones we needed. Tracing problematic incidents meant searching outside of the browser for clues in the network or on the endpoint. Malicious files were only scanned and detected once they left the browser, when it may already be too late. Our analytics platforms collected at-best an incomplete view of organizational activity.

But with the Enterprise Browser, your security stack is now integrated into the browser, instead of locked out. Your entire security stack can see all user activity and data first-hand, making them instantly smarter, while making their jobs simpler. Data Loss Protection makes smarter real-time decisions about which files should or shouldn't be downloaded - before they even leave the browser.

Malware scanning is integrated into the browser, protecting the organization from ransomware or zero-day exploits at the very place they arrive. Firewalls identify and block security risks inside the browser itself, so they know exactly what threats to keep away from your network or endpoint. And analytics platforms finally have a comprehensive view of everything happening inside the organization, enabling you to gain more accurate insight and make more sound decisions.

The Use Cases

By sitting at the epicenter of enterprise work, The Enterprise Browser has the potential to fundamentally solve use cases of all kinds.

With the Enterprise Browser, you can set highly specific policies to govern which applications and data contractors can access from inside the browser itself.

Critical SaaS Applications

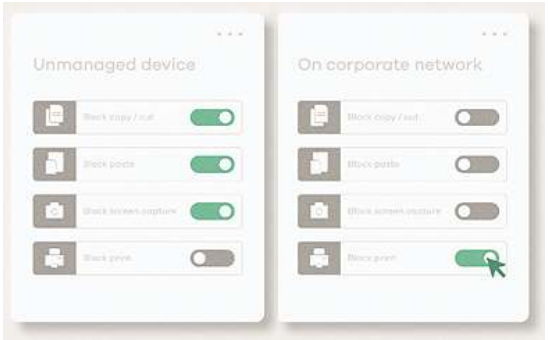
Aside from their limited built-in security controls, it's been virtually impossible to govern and secure the data accessed inside the SaaS and internal web apps core to enterprise work today. But with Island, organizations finally have a closed-loop system inside which granular policies can be implemented across all SaaS and internal web apps, ensuring the data inside them remains fundamentally secure, without relying on limited and complex network controls, disparate app-specific APIs or other limited solutions.

Bring Your Own Device (BYOD)

As the use of unmanaged devices for work has become mainstream, the risk of sensitive data leakage has become a constant challenge with no comprehensive solution. With the Enterprise Browser, organizations can finally offer this level of professional freedom without compromising on security whatsoever. With Island, users work freely on any device they choose while accessing critical data via a browser designed to keep it where it belongs.

Contractor Access

Enterprises regularly need to give outside contractors access to critical applications. But doing so means sharing highly sensitive applications and underlying data with users and unmanaged devices the organization can't see or control. With the Enterprise Browser, you can set highly specific policies to govern which applications and data contractors can access from inside the browser itself. You can also audit the usage of those apps and data to make sure all activity is as it should be. And most importantly, by provisioning their work from inside the browser, all the typical IT friction is gone - positioning contractors to work quickly and efficiently.



Privileged User Access

Most applications require accounts with highly specific privileges for organizational management needs. Yet who is watching and governing the use of these privileges? These accounts become easily prone to misconfiguration or sabotage. Island uniquely protects privileged user accounts by adding deep forensic logging on transactional events, forensic screenshots of key actions and even multi-factor authentication on top of any key action, ensuring no unauthorized action takes place - accidental or otherwise.

Virtual Desktop Infrastructure (VDI) Reduction

As organizations have raced to embrace work-from-home policies in response to the global COVID pandemic, many have turned to costly VDI solutions to provide browser access to critical applications for off-premises users. Island completely removes the overhead of VDI management and licensing costs for governing access to critical web applications for remote users, while providing a significantly more fluid and familiar experience users expect from a browser.

Say 'Yes' to Consumer or Risky Apps at Work

Organizations often forbid the use of consumer applications to avoid the transfer of corporate information into one's personal email or messaging accounts, for example. With Island, organizations can actually 'say yes' to applications that challenge their security posture by setting policies that ensure no sensitive corporate data will be able to leak onto them.

About Island

Island, the Enterprise Browser is the ideal enterprise workplace, where work flows freely while remaining fundamentally secure. With the core needs of the enterprise naturally embedded in the browser itself, Island gives organizations complete control, visibility, and governance over the last mile, while delivering the same smooth Chromium-based browser experience users expect. Led by experienced leaders of the enterprise security and browser technology space and backed by the world's leading venture funds -- Cyberstarts, Insight Partners, Sequoia and Stripes -- Island is redefining the future of work for some of the largest, most respected enterprises in the world.

Island

Sometimes changing one thing changes everything.

3501 Olympus Blvd. Suite 350
Dallas, TX 75019
(866) 832 7114
info@island.io