Island

The Evolution to a Browser Built for the Enterprise:

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

White paper | August 2023

Executive Summary

The browser is the most commonly used application in the enterprise.

Consumer browsers such as Edge and Chrome weren't originally designed as an enterprise application. At their core they are simply vehicles to render web content. In the enterprise context, at best they have rudimentary settings that are centrally controllable, but no sophisticated policy to protect corporate applications, the underlying data, and the user. Unsure of this? Just examine the security stack surrounding the typical browsing experience; organizations continue to deploy a complex and expensive series of technologies around these browsers that are challenging to manage and frustrating to work with for users and security teams alike. Island is the world's first Enterprise Browser that naturally embeds many of the core needs of the enterprise into the smooth, familiar browser experience.

Unlike these traditional browsers, Island is contextually aware of the environmental factors it is operating within (user, groups, geolocation, network, device awareness, etc). By using such contextual clues, the organization gains complete control over the last mile, with the ability to govern and audit all browser behavior and customize the browsing experience to support every workflow. Browser activity data is collected and centralized, radically improving the effectiveness of the entire infrastructure. Or, complete user privacy can be asserted in other situations. This approach can fill in the missing puzzle pieces of a zero-trust initiative to ensure a natural fit for an evolving workforce and 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 endpoint, BYOD and contract workers get to work without putting data at risk or adding layers of virtualization, user credentials are now safe from phishing or inappropriate re-use, users are protected from malicious content, consumer apps are now safely permitted inside the workplace, and much more.

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

Introduction

The most-used application wasn't designed for the enterprise.

Despite universal adoption by enterprises everywhere, the browser isn't 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-is. Upon its arrival in the enterprise, we realized that it might be useful to centrally manage the rudimentary settings of the browser via things like GPOs or other clunky management tools, but very little has happened to make the existing browser ready to operate within the enterprise context.

Since browsers such as Chrome and Edge were never designed for the enterprise, they lack 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 unable to leverage the one application our organization depends on most and instead must work to neutralize it.

Because the browser doesn't cooperate with the enterprise, we're given no choice but to surround it with gateways, CASBs, DLP solutions, firewalls, and an endless array of security solutions. In the process, the technology stack becomes complex, expensive, and fragile to maintain. Further, our users suffer in the process through unnatural experiences where controls get in the way or technologies such as desktop virtualization and remote browser isolation create unnecessary friction. We're forced to make painful tradeoffs that leave our organization too exposed or users too confined.

And we're still blind to what's actually happening in the browser. We're unprepared to protect the most critical resources our organizations hold dear. Ironically, the reason we chose the browser in the first place — its smooth end user experience and universal usability — 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 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.

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 work happens, while delivering the same smooth Chromium-based browser experience users expect.

With a browser built to cooperate with the enterprise, everything around it gets smarter, simpler, and easier. Files are now scanned for data loss, malware, and other security policies before being downloaded, uploaded, or viewed. User identity and device posture inform access privileges, with direct access to SaaS applications and secure connectors allowing for native private app access without a VPN. Credentials are protected against inappropriate reuse or malicious phishing attempts. Every web request is checked for risk and category-based safe browsing rules. And all the detailed browser activity is fed directly into your SIEM or other analytics platforms, completely avoiding the complexities of decrypting and inspecting SSL traffic over the network. Because it's a browser, policies are enforced locally for unmatched performance and dramatically simplified infrastructure requirements. Things the consumer browsers are simply unable to do.

Yet Island can sit alongside your existing consumer browser such as Edge, Chrome, Safari, etc. while being enforced for critical applications and activities that require maximum control, governance, or visibility. Or it can serve as your primary browser for all web activity, providing deep protection for the user and the browser even on an unmanaged device. 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 the 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, leveraging security tools like sandboxes, remote browser isolation, VPN, endpoint agents, or virtual desktops comes at the cost of the end-user experience. This may cause users to resist their adoption.

We understood in order for the Enterprise Browser to be implemented and actually adopted, it cannot come at the price of the end-user experience. That's why we built the Enterprise Browser using the open source Chromium project: the same technology that powers Google Chrome, Microsoft Edge, and many others. Chromium delivers the core services of user experience, rendering, JavaScript interpretation, extensions, and networking. Which means users will have an experience identical to the browser they use today — thus requiring no training or effort to gain user acceptance.

Securing the Last Mile

At the heart of any enterprise application is the means to adeptly 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. Thus we "wrap" that browsing experience with host-based agents, remote browser isolation, proxies, DLP, CASB, SASE, and many other technologies to govern what takes place within the browsing window.

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 preventing a user from copying and pasting sensitive data into something like personal Gmail or another application? Yet how do we empower them to do so into the corporate tenant of the same 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 within the same app?
- How do we stop one group of users 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 help ensure privacy adherence when consumer browsers share consumer data with third party browser suppliers?
- How do we ensure a safe experience even when users aren't on a managed network or VPN?

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, geolocation, network connection, application tenant 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, specific tenants of an application, and external destinations
- Screen captures of critical application areas
- Printing application pages
- File download or upload within an application
- Adding multi-factor authentication to certain areas of an application
- Redacting sensitive on-screen data without any backend code changes
- Watermarking to discourage phone or camera screen capture
- Redirecting downloads to the organization's secure storage (e.g., OneDrive, Google Drive)

These are just some of the countless examples of how the Enterprise Browser protects the data inside critical applications. This approach is fundamentally different from consumer browsers that allow unfettered access to the application data once it reaches the browser.

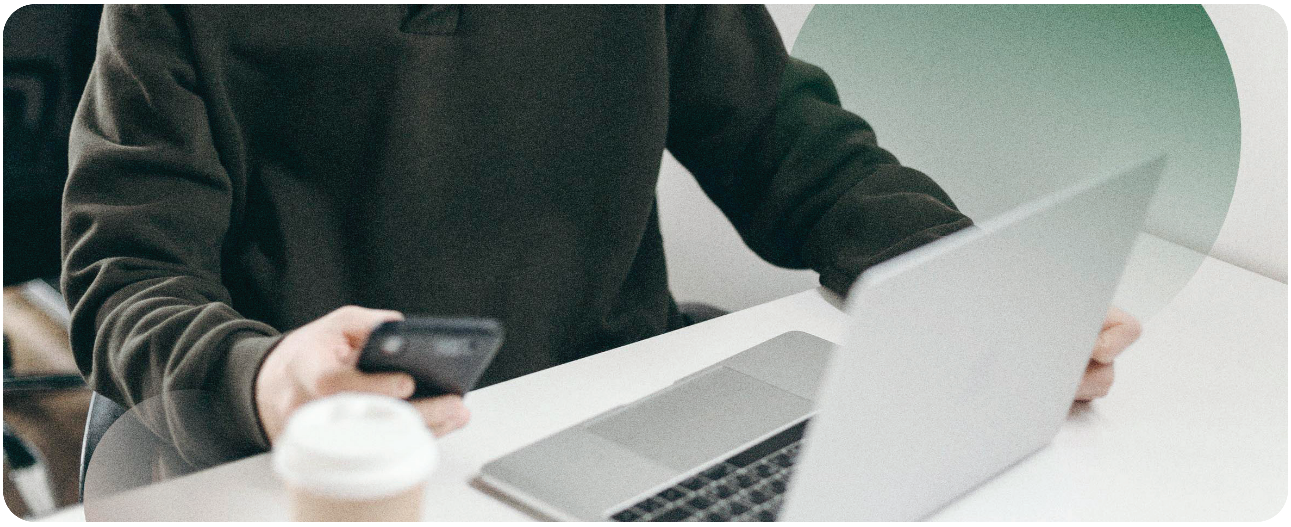
Auditing and Logging Browser Activity

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, 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 outside the browser, but never seeing the full picture itself. This is simply due to the fact that the consumer browser was never designed with enterprise visibility in mind, and does not cooperate with enterprise visibility tools in any meaningful way. Further visibility is often achieved through the unnatural act of breaking open the SSL traffic since mechanics do not exist in consumer browsers for such audit needs.

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 high fidelity. You can even capture mouse clicks, a screenshot or even keystrokes of a privileged application area or a full step-by-step timeline of user interactions to have visual proof of critical interactions. At the same time, some user engagements require anonymous logging or even fully private browsing. Island is contextually aware and policy-driven to support the full range of visibility. This helps organizations dynamically ensure a greater set of capabilities where geopolitical issues exist around data privacy laws. Dynamic behavior such as this based upon the contextual need sets Island apart from any consumer browsing experience.

The Island management console provides a detailed timeline of events that is easy to read and understand. In addition, Island can feed browser activity data to your existing SIEM or other analytics tools, giving a level of visibility that was simply not possible before. Security teams benefit from seeing the complete picture of all user activity, in context, so they can take action and keep the organization secure.



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, and the starting page with all your enterprise apps & resources. Inform and engage with users by tailoring browser notifications and messaging. Tailor web apps (even third-party apps) to fit your needs by adding robotic process automation (RPA) modules that modify applications within the presentation layer of the browser. No source code changes required.

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

For apps that don't support SSO, or where shared credentials are required (e.g. Twitter), the Enterprise Browser offers secure credential access. For authorized users, the browser will inject credentials at the login page — without ever disclosing the password in plaintext. When it's time to rotate passwords, simply update once in the Island management console. And since all web activity is logged, you have an audit trail for every time the credentials are used.

Simply put, these capabilities do not exist in the consumer browser landscape even when centrally managed.

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 prevention (DLP) 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 an incomplete view — at best — 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. DLP 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, along with native browser isolation techniques, protecting the organization from ransomware or zero-day exploits (such as attempts to inject malicious code into the browser) at the very place they arrive. Web classification is done within the browser to block or warn about risky or inappropriate destinations. Advanced extension management gives you granular control over browser extensions to balance user productivity and convenience without compromising on security. 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 center of enterprise work, the Enterprise Browser has the potential to fundamentally solve use cases of all kinds where consumer browsers are unable to answer the need.

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.

Virtual Desktop Infrastructure (VDI) Reduction

As organizations have embraced flexible remote-working policies, 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.

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 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.

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.

Private Apps or Semi-private Cloud

Organizations often turn to VPN for connecting to private apps hosted in a data center or semi-private cloud. Backhauling network traffic over VPN is inefficient and can add security risks. The Enterprise Browser offers a much simpler and secure solution for connecting to private apps or semi-private cloud. Island can make use of existing network infrastructure or augment with per-app connectors to secure traffic between private apps and the browser. All without opening the external firewall or backhauling traffic over VPN.

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.

Say ‘Yes’ to Consumer or Untrusted 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 is the developer of the Enterprise Browser — 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 leading venture funds — Insight Partners, Sequoia Capital, Cyberstarts, Stripes, Cisco Investments and Georgian — Island is redefining the future of work for some of the largest, most respected enterprises in the world.