Brought to you by Informa Tech
OMDIA

Publication date:
09 Feb 2023
Author:
Rik Turner, Senior Principal Analyst

On the Radar: Island offers an enterprise browser for security and productivity gains

Summary

Catalyst

Island pioneered the development of enterprise browser technology, which delivers security to organizations via a browser that their IT and SecOps teams can use to define usage policy for employees and contractors in a way that is not possible with the standard browsers that ship on endpoint devices. While it debuted with a product that focuses on a security use case, the vendor sees the potential for significant transformation within broader IT use cases while empowering productivity assistance for developers, admins, and general business users.

Omdia view

The days when apps lived on users' desk- or laptops or even in the "computer room" at the end of the office are long gone, and while some may still reside physically in a corporate data center the trend is clearly for them to be in the cloud. In the case of a private app written by an organization for its employees, this will be a private environment such as a VPC in AWS or a VNet in Azure, while for software as a service (SaaS) apps, it is the public cloud.

In either case, threat actors and even malicious insiders see opportunities to leverage the consumer browser as a point of weakness, and for this reason the security industry has been paying an increasing amount of attention to this vector in recent years. Island is in the forefront of efforts to address it and is well positioned to gain significant share in the still evolving browser security market.

Island sees the browser as the first point at which users engage with critical applications and data, and as such it must be protected from accidental abuse, insider threats, and malicious actors. Its goal is to avoid replaying the sins of the past and being lumped into a "secure browser" market, casting itself as a broader player with a platform that enables security plus other benefits with the use of its browser.

Why put Island Enterprise Browser on your radar?

The Island Enterprise Browser can replace the standard browser on a user's laptop or can coexist with it, and in either scenario it enables ITOps to define acceptable policy for what users can and cannot do with corporate information. It also isolates the user's corporate browsing activity, avoiding browser infections that can lead to data exfiltration. Finally, it can be deployed via a local install process and represents minimal management overhead vis-à-vis conventional browsers.

What makes Island particularly interesting, however, is its vision of its browser fulfilling roles beyond security, aiding productivity across a range of enterprise roles.

Market context

The enterprise browser market is an emerging technology segment that recognizes the real estate of the browser as a key vehicle to protect an organization's key resources within its applications while at the same time making sure users can operate safely. And of course, the case for such an approach has only grown in strength, now that corporate employees spend so much of their time in SaaS or the so-called private apps written by organizations for their staffers to access in infrastructure- or platform-as-a-service (IaaS or PaaS) environments.

In this scenario, the browser has the potential to become a vehicle for protecting critical applications and the corporate data that traverses them, as well as underpinning new work paradigms such as hybrid work, contractors, BPO, and so on.

Since all these apps are accessed via a browser, being able to compromise that line of communication is invaluable for threat actors. If they can infect the browser with a Trojan, for instance, they can learn all about the user's destinations on the internet and use that knowledge for a wide range of attacks, from theft of intellectual property to raids on online bank accounts. Such exploits are known as man-in-the-browser (MitB) attacks, as well as so-called boy-in-the-browser (BitB) attacks whereby the malware makes changes to a target machine's routing (often by changing an operating system's hosts file), then deletes itself.

Browser isolation

To address such challenges, there has been a range of responses from the security industry. First came browser isolation technology, which places each browser session in a separate virtual machine that isolates it from the underlying infrastructure, including the machine's BIOS and operating system. Two flavors of this technology emerged:

- One carried out the isolation on the endpoint (so-called local browser isolation or LBI). This approach was championed by a vendor called Bromium, which is now part of laptop manufacturer HP. It had significant limitations at the time, however, because first, it was quite compute-intensive, taking CPU cycles away from the enterprise apps the user was working in, and second, the technology could only be deployed on more recent generations of x86 processors, so if your company had a mixed estate with older endpoints, Bromium was only a partial solution to your security problem.
- The other approach, called remote browser isolation (RBI), performed the same function on a server and presented a sanitized version of the webpage to the endpoint. This approach was more popular due to the shortcoming of LBI outlined above. Several RBI vendors emerged

including one founded by Dan Amiga before he founded Island. Many were acquired with the best-known dedicated RBI vendor still in existence being Menlo Security.

Island notes, in this context, that neither of these approaches was designed to protect critical application usage or the underlying data. Rather they were developed to protect enterprise users from bad actors who had compromised websites.

Changes to the browser

More recently, the focus has shifted to making changes to the actual browser, and here again, two distinct approaches have emerged:

- Firstly, there are vendors who propose an extension to the existing browser, injecting extra intelligence in the form of lightweight JavaScript that enables the security and manageability that is missing from standard browser technology.
- The second approach is the development of a completely new browser. This "enterprise browser" can either live alongside the standard one on the endpoint and be used for all corporate activity, leaving the other one for the user's personal browsing, or can completely replace it and be used for all the browser activity from that machine.

Island was the first vendor in the second of these categories, and indeed it coined the name enterprise browser.

Product/service overview

Enterprise browsers propose the use of different, purpose-built browsers through which organizations can enforce their security policies and thereby avoid infection or other forms of compromise by threat actors. They can either replace altogether the consumer browsers that ship as default on desk- and laptop machines or they can coexist with them with the endpoint configured in such a way that any corporate internet use is forced through the enterprise browser, while personal surfing can still go through the regular one.

For convenience and reduction in development costs, enterprise browsers take as their basis the most widely used codebase in the market, namely that provided by the open-source Chromium project developed and maintained by Google. They then added in their own features, which include integration with the customer's identity provider, such as Okta or Azure AD, as well as with their provider of SSO services.

Enterprise browsers can thus rely on Chromium for updates to its part of the technology, while the browser vendor takes care of updates to the functionality they have added. For the latter, the Island Enterprise Browser actually "phones home" to get any updates to the vendor's part of its functionality.

As the company that came up with the concept, Island uses the name of the emerging category in its product, calling it the Island Enterprise Browser. Its installation on the devices of individual employees or contractors can be as a package deployed by the IT department, or the end user can be directed to a download page for the purpose, with Island enabling IT admins to set the timeline and deadlines for the install. The actual installation requires no admin credentials. Once the Island browser is in place, it merely requires a restart of the machine to begin operating with the policies set by ITOps.

Browser replacement vs. coexistence

Island refers to the scenario in which its browser replaces standard Chrome, Edge, or Safari on the endpoint as the full browser use case, which is favored by the most security-sensitive organizations. The other more-common one is where it lives alongside the standard browsers and any engagement with a corporate application is forced through the Island browser. Island has created several vehicles for enforcement of its browser both in managed and unmanaged environments. This type of deployment is also useful when third-party contractors, potentially bringing their own mobile devices, are operating in a corporate environment.

When an employee has been redirected to the enterprise browser to access a particular app, Island Enterprise Browser can retain their credentials thanks to integration with the IdP, and thus can log in on their behalf. In the case of a third-party contractor, on the other hand, it can offer a pop-up screen that requires the individual to fill in the appropriate identity information, while the browser itself keeps the login credential secret from the user, who is logged in once they have filled out the appropriate pop-up information.

Graying out sensitive data

Island also has built security into its platform for the browser coexistence scenario. If a user has both the Island and a regular browser open at the same time, policy governs what they can and cannot do on the corporate app side. Thus, whenever they switch across to the consumer browser, the data fields on the pages viewed with the Island browser are automatically grayed out such that they cannot cut and paste information from within the enterprise browser session to a page being viewed by the regular one. Island has invested considerable resources to deliver the kind of policy dexterity that can handle such user interactions gracefully.

Company information

Background

Island was founded in 2020 by CEO Mike Fey and CTO Dan Amiga. Fey was previously President and COO of Symantec before which he was COO of Blue Coat Systems (acquired by Symantec in 2016) and before that was GM and CTO of McAfee. Meanwhile Amiga was founder at CTO of Fireglass, a remote browser isolation (RBI) company acquired by Symantec in 2017. He was also a founding investor at various companies, including secure service edge (SSE) vendor Axis Security, Build Security, which offered a permissions policy management platform for developers (acquired by Elastic in 2021), and software supply chain security vendor Cycode. He also holds positions at Israeli VCs Cyberstarts and YL Ventures.

Island has raised a total of $285m to date, most recently announcing (in November 2022) a $60m extension to its $115m Series B round from March the same year. The first tranche of the Series B was led by Insight Partners, while the leader of the second was Georgian Partners. Notably, that Series came only a few weeks after a $100m Series A round, also led by Insight, which coincided with Island's emergence from stealth.

Current position

Island's current target market is the enterprise segment, though it is already thinking about going down-market (see **Future plans**). It has customers with as many as 100,000 users but says it already has some with as few as 500. The charging mechanism is per user rather than per device such that the same user can use

the enterprise browser across multiple devices. There are already versions of the browser for iOS, iPadOS, and Android as well as for Mac OS, Windows, and Linux.

In response to requests from the healthcare sector where health professionals typically work on multiple machines across their working day, Island added a feature in late 2022 whereby each instance of its browser can have multiple user profiles on it so that different individual workers can log in and use the same machine at various times of the day.

In late 2022, Island launched Island Private Access, which was designed specifically to address the requirement for browser access to private rather than SaaS apps. The service comes with a cloud-based management console for the customer who takes Private Access.

In January 2023, meanwhile, the vendor announced Island GPT Assistant, which is an integration of ChatGPT's AI technology into the browser enabling users to ask it for all kinds of help such as providing a summary of the key points of an email, scanning code for bugs, or coming up with suggestions for the perfect title for an email.

Island's competitive landscape is a variegated one, in that there are competing technologies such as RBI and browser extension as well as direct enterprise browser competitors. As the first out of the gate in the last category, however, Island feels it has a lead over the other vendors in the space, while against the competing technologies it can point to clear advantages in functionality.

Future plans

Island sometimes refers to its Enterprise Browser as a platform disguised as a browser, a description that was first used by a happy customer, and which is indicative of how the company is thinking about the future of its technology. The integration with ChatGPT is further evidence that Island has plans for its product that go beyond security. If the browser can learn a user's work patterns, for instance, it could start to make recommendations of smarter ways to get things done.

This would have relevance in, say, a software development environment. The Island browser might proffer suggestions for how the code could be more secure or more efficient.

Key facts

Table 1: Data sheet: Island

Product/service name	Island Enterprise Browser	**Product classification**	A browser that enables security for corporate data and infrastructure
Version number	N/A	**Release date**	February 2022
Industries covered	All	**Geographies covered**	Global
Relevant company sizes	Enterprise	**Licensing options**	Per-user subscription
URL	www.island.io	**Routes to market**	Direct and channel
Company headquarters	Dallas, Texas, USA	**Number of employees**	Undisclosed

Source: Omdia

Analyst comment

There is no doubt that the browser is now a prime target for threat actors, and browser security has gained in importance as a result. The enterprise browser segment is among the more recent approaches to address the challenges of browser attacks.

As a relative newcomer in the market, its purveyors must first educate the market as to what the technology is, how it works, and, crucially, how it is deployed and managed. There is considerable FUD from competitors in the browser extension market that argue that it is much easier to just add the extension to one's existing browser, losing none of the management features of the standard browsers from the likes of Google and Microsoft. It behooves the enterprise browser vendors to demonstrate that their products are not only more secure, but also that deploying them entails no additional management overhead, nor a loss of manageability vis-à-vis regular browsers.

It will be interesting to see whether any of the enterprise browser vendors are acquired by larger, more diversified security companies, as happened with some RBI startups. Such a development would certainly provide validation for the technological approach, while at the same time changing the competitive landscape, if the incoming buyer was a tech heavyweight with a large marketing budget.

As things currently stand, Island has only other startups to compete with in the pureplay enterprise browser market. As a result, it needs to raise the profile of the technology itself as well as establish its credibility as an enterprise tech provider. Clearly, it has benefitted from the profile of some of the members of its executive team, many of whom have between 15 and 25 years' experience in cybersecurity, with resumés that include exec roles at major players in the sector.

Omdia finds particularly compelling Island's vision of its enterprise browser as incorporating other features to bring further value to its customers beyond the security capabilities it has so far focused on. The integration with ChatGPT is clearly only the first step in this direction. Island Enterprise Browser as a

platform for security and productivity improvement is an intriguing notion that makes the vendor worth following as it develops its ideas.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Omdia Universe: Digital Workspace Management / Unified Endpoint Management Platforms, 2023 (December 2022)

Omdia Market Radar: Endpoint Security Platforms (August 2022)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com