OMDIA MARKET RADAR

Publication date
August 21, 2023

Author
Rik Turner, Senior Principal Analyst Cybersecurity
Rob Bamforth, Associate Analyst, Cybersecurity

Browser Security 2023

OMDIA

Brought to you by Informa Tech

Summary

Catalyst

After a decade or more in which browser security was limited to a single approach—remote browser isolation (RBI)—the 2020s have seen a flowering of new and different approaches to the problem. An oversimplistic categorization of these techniques puts them into two groups: browser extensions and enterprise browsers, as will be explained below. However, closer inspection reveals a whole spectrum of approaches each subtly different from the next, and each with its strengths and weaknesses.

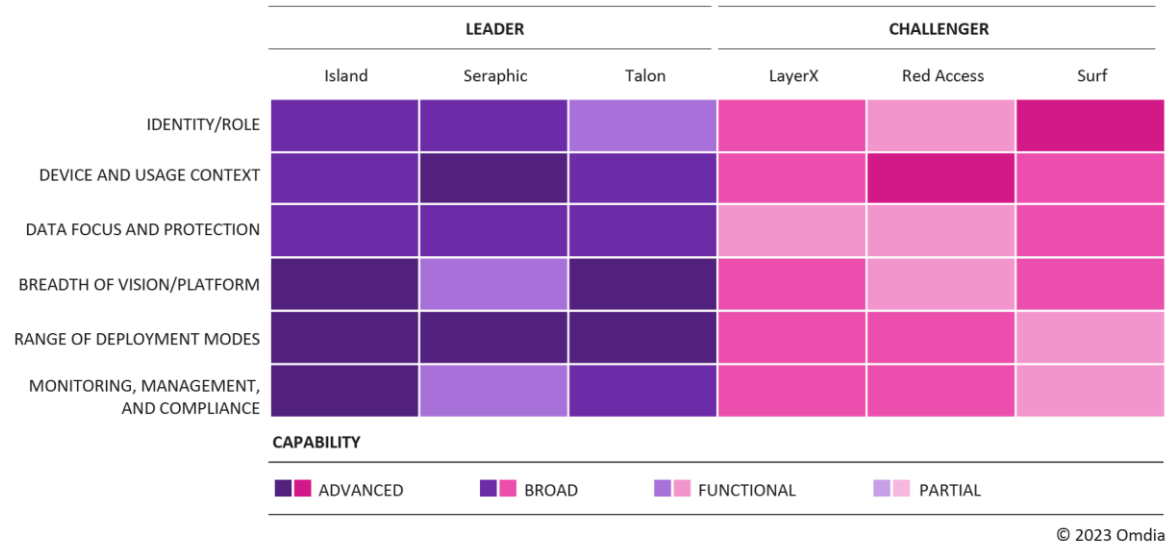
This report sets out to catalog the main players in this evolving landscape and, in a coarse-grained manner, to indicate those that Omdia believes are more advanced in their product and business trajectory. We explain why browser security has gained in importance of late, as evidenced by the amounts of funding that have flowed into some of the vendors profiled here, and venture to suggest where this emerging category could be going in the years ahead.

Market snapshot

In this Market Radar, Omdia explores the various approaches to achieving browser security. Trends such as the adoption of cloud computing and the move to hybrid work have raised the need to secure the browsing activity of corporate employees and contractors. The concern was initially centered around inbound traffic. This means the risk of someone visiting a website that sends malware to a device, from which it could access and subsequently exfiltrate sensitive corporate data or wreak havoc on a company's IT infrastructure. More recently, as software-as-a-service (SaaS) application use has proliferated through enterprises, the focus has expanded to outbound traffic, addressing insider threat as well as the account hijack scenario.

This report compares the different approaches, as well as the various vendors in this category. It considers the pros and cons of each of the approaches, describes a somewhat more variegated technical landscape than the simple dichotomy of extensions versus enterprise browsers would suggest, and looks at the strengths and weaknesses of the individual providers.

Figure 1: Omdia Market Radar on Browser Security, 2023



Source: Omdia

Key messages

- The browser is now a prime target for cyberattacks.
- Cloud means browser attacks now bring even richer pickings.
- Browser-based exploits are multifarious.
- Some exploits don’t even target the browser directly.

Recommendations

Recommendations for enterprises

Familiarize yourself with the various approaches to browser security

You may already be familiar with RBI, but if not then understand how it works and where it might be appropriate in your organization, then study the more advanced approaches of browser extensions and enterprise browsers. As explained below, each has positives and negatives, and you will need to gauge which is best for your particular situation.

Be prepared to mix and match

No two enterprises are identical. If you have a lot of people within your organization working on noncorporate-owned devices, for instance, this will affect the kind of browser security you can offer them. There is no need to go for one particular approach. Obviously, deploying technology from different vendors can complicate matters from a management perspective, but Talon and Seraphic, for instance, already offer flexibility in how their security capabilities are delivered, and if you particularly like another vendor's tech, ask them whether they too are planning to vary their deployment methods, or even their product portfolio, in the near future.

Quiz your secure access surface edge (SASE)/secure surface edge (SSE) provider on its plans for browser security

If you are already a customer of a SASE provider, it is very likely by now that it already offers RBI as one of the capabilities of its platform. If you want to go further with browser security, however, you should ask it whether it might offer extensions or even enterprise browser technology, either through internal development or by partnering with one of the specialist vendors profiled in this report.

Recommendations for vendors

Invest in market education

While the browser security market has been recognized by venture capitalists as a worthwhile target for their investments, many potential customers may still be largely unaware when it comes to the finer points of how newer technologies work in this sector. There are a number of myths that need dispelling, such as the idea that an enterprise browser can only work by being the exclusive browser on an end user's device, or that a regular consumer browser on the device cannot be controlled and is thus a security loophole. Similarly, browser extensions are not so easily circumvented as their detractors suggest. All of this requires market education initiatives.

Don't criticize a competing approach: you may end up offering it

While tech marketing inevitably highlights the shortcomings not only of competing vendors but also of their technology, you may find that as this market evolves your company will see the benefit of

launching a product in the competing category to fill out its portfolio. So avoid going too far in deriding another technical approach lest you find yourself contradicting yourself later.

The browser is now a prime target for cyberattacks

While the human eye is the organ we use to see the world around us, there is a well-known expression that the eyes are "the window to the soul." In other words, looking into someone's eyes can reveal a lot about their personality.

In a similar manner, the browser is the tool that an organization's employees use to "see out," not only onto the web but also and increasingly into the applications that they use to do their jobs. These can be SaaS apps like Salesforce and Microsoft 365, as well as the so-called "private" apps that are housed in infrastructure- or platform-as-a-service (IaaS/PaaS) environments and developed by their employer to enable specific functionality relevant to their business.

And just as the eyes may be used to read a person's character, so the browser can be harnessed by threat actors to look into the data, infrastructure, and corporate structure of an organization. As more companies adopt cloud computing to power their digital transformation initiatives, the browser has become the default mechanism for accessing enterprise applications, with all that this implies for the organization's security posture. Compromising a browser can convert it into a window, if not onto the soul, then at least to the brain and accumulated knowledge of an organization. Browser-based attacks can enable the injection of malware, the exfiltration of sensitive data, and many other types of cyber exploit.

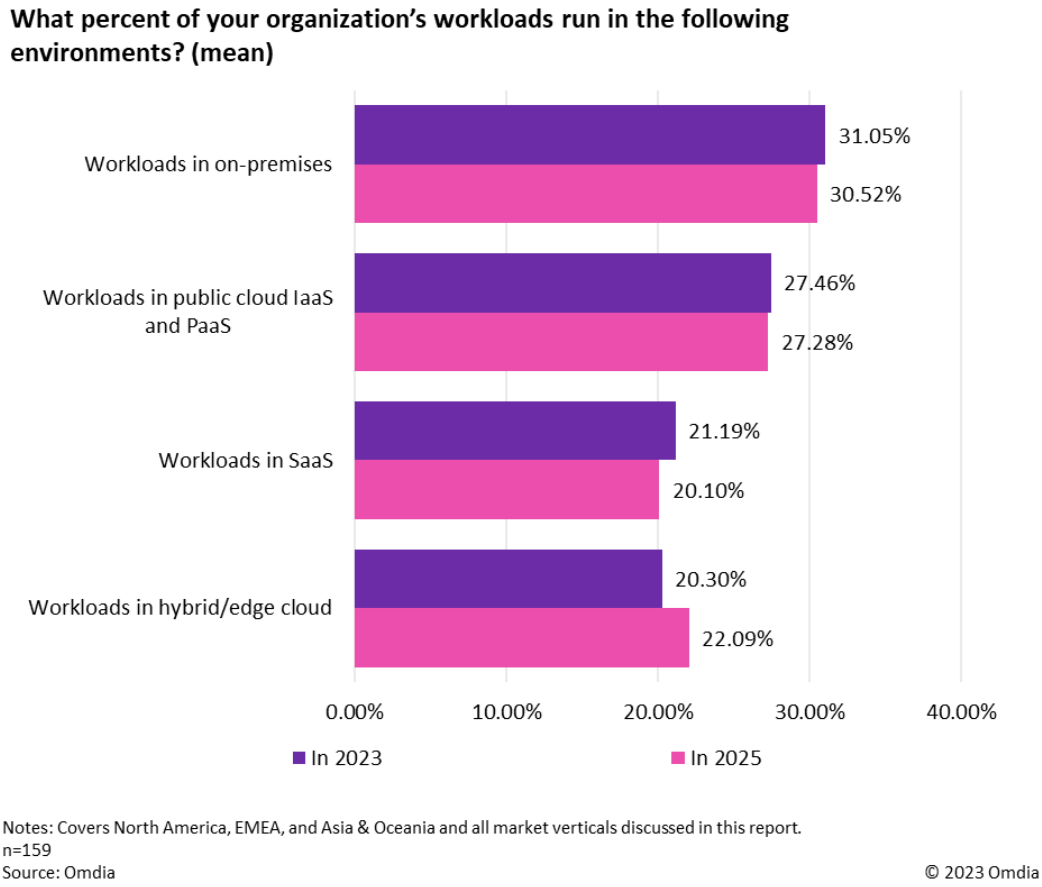
Cloud means browser attacks bring even richer pickings

Attacking the browser has been a favorite modus operandi ever since the web became a valuable information tool for businesses. However, over the last decade the incentive to mount such attacks has increased dramatically.

Firstly, corporate employees spend increasing amounts of time on SaaS platforms, or in the private apps written by organizations for their staffers to access in IaaS or PaaS environments. In other words, robbers now have the prospect of a much richer haul.

Figure 2 is taken from Omdia's annual *Cloud Services End-User Survey* for 2023, which had 159 respondents from organizations of all sizes in the three biggest business regions of North America, EMEA, and APAC. It shows that just under 70% of workloads are running in some form of cloud today (public IaaS or PaaS, SaaS, hybrid, or edge) and that the trend is for a slight increase by 2025. Numbers were higher for the large enterprise segment.

Figure 2: The cloud is the dominant locus for workloads

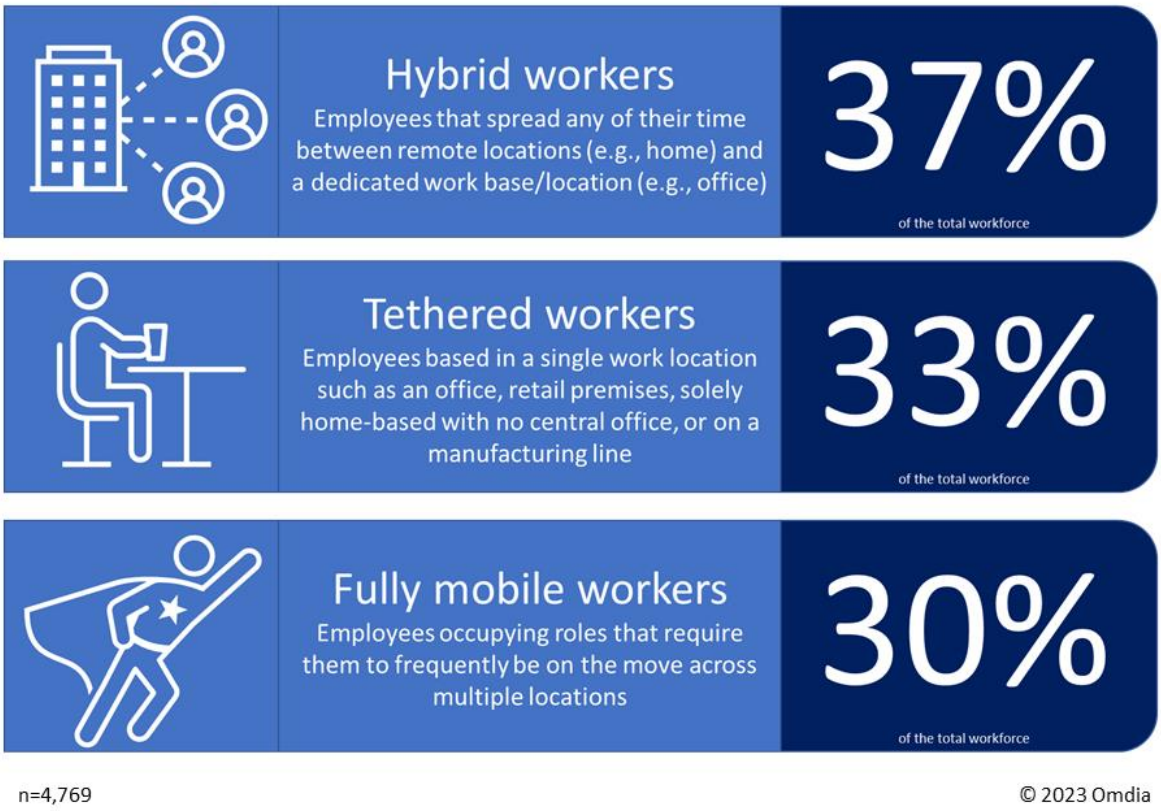


Notes: Covers North America, EMEA, and Asia & Oceania and all market verticals discussed in this report.
n=159
Source: Omdia

Source: Omdia

Secondly, more employees are working remotely, increasing their dependence on browser-accessed applications while at the same time reducing their IT department's ability to control and secure their browsing activities. **Figure 3**, compiled from an annual survey conducted by Omdia into changing workplace habits, is indicative of this trend.

Figure 3: Work styles have become more mobile/remote



Source: Omdia

Browser-based exploits are multifarious

There are by now a multitude of types of attack against browsers, as threat actors come up with ever-more-ingenious ways to exploit them for their own ends. For instance:

- If they can infect a browser with a Trojan, 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. Famous examples are Zeus, Spyeye, Bugat, Carberp, Silon, and Tatanga.
- A sneaky variant of MitB are 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, and then deletes itself. Mobile browsers have also come under attack via man-in-the-mobile (MitMo) attacks such as Zeus-in-the-mobile (ZitMo) and Spyeye-in-the-mobile (SpitMo).

- Another well-established attack path is **SQL injection**, which corrupts web forms, cookies, or HTTP posts and uses them to inject their malicious code into a visitor's browser, which will execute the code because it considers it as coming from a trusted source.
- Another type of attack uses so-called **malicious browser plug-ins**. There are, of course, thousands of legitimate plug-ins (a.k.a. extensions) that add useful functionality to web browsers such as blocking ads, disabling JavaScript, or downloading YouTube videos. However, by virtue of the fact that to deliver such functionality a plug-in requires full access to a user's browsing history and needs to be able to manipulate traffic, there is an incentive for bad actors to develop malicious plug-ins with functionality that goes beyond what the user downloads.

Some exploits don't even target the browser directly

It is also the case that many attacks don't need to target the browser directly at all. Instead, they go after particular web applications or websites, with the browser being used as the vehicle for delivering the malicious payload. Examples of such attacks are:

- **Cross-site scripting** (XSS), the most common, uses the application or website to deliver malicious client-side scripts to a user's browser. This executes the script without user intervention. Once executed, the script can do a variety of things including exfiltrating personal and financial information from the site, installing malware, or redirecting the victim's browser to other malicious web pages.
- Without requiring any actual change to the browser, another form of attack is **session hijacking** whereby an unencrypted or poorly encrypted session ID between a web server and an end user's device is intercepted, enabling the malicious actor to start a new, authenticated session in the original user's name. Browsers connecting to unprotected public hotspots are particularly vulnerable to such attacks.
- **DNS poisoning** is another type of attack that affects the browser without actually touching it, either by compromising a DNS server or by poisoning a local DN cache. Both approaches will have the same effect of directing the browser to a compromised website, instead of the legitimate one requested, for the purpose of harvesting the user's personal data.

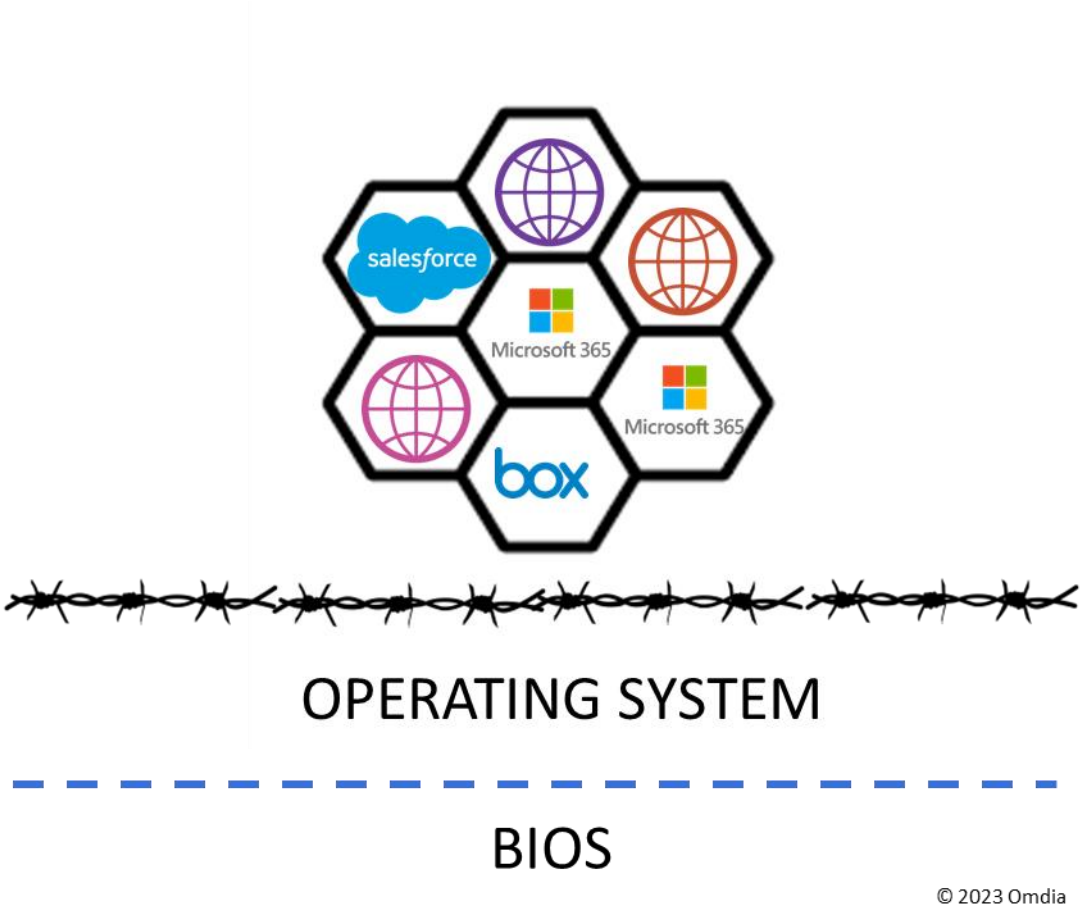
Browser isolation

To address the burgeoning field of browser-based attacks, a variety of approaches have emerged over the last decade or so. First came browser isolation technology, which places each browser session in a separate virtual machine (VM) that isolates it from the underlying infrastructure, including the machine's BIOS and operating system.

RBI can be traced back to 2010, when the first implementation of this approach to web security came onto the market. Rather than making a dramatic splash with huge uptake, the technology has since enjoyed fairly steady but unspectacular growth, picking up committed customers without making any of its proponents into unicorns.

In parallel, several broad-based vendors in network security have acquired RBI specialists in recent years, so while the technology has largely disappeared as a standalone offering from dedicated vendors, it is very much present as part of broader security portfolios, bundled into either a SASE or an SSE.

Figure 4: Browser isolation: putting each browser session in a separate VM



Source: Omdia

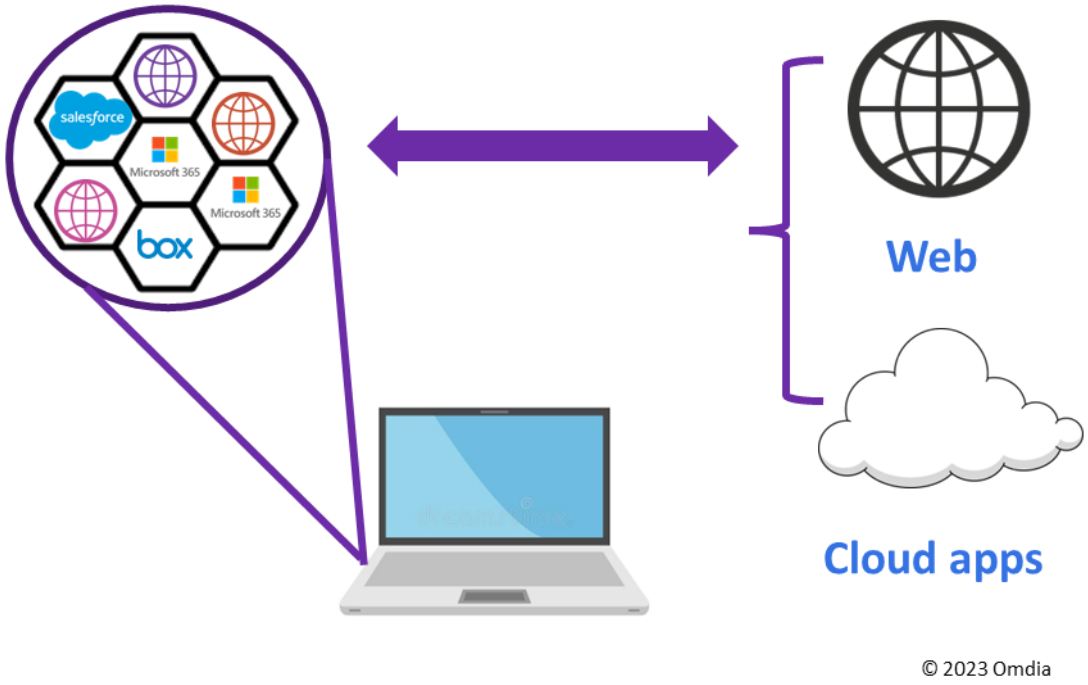
Local browser isolation (LBI)

Two flavors of isolation emerged. One carried out the isolation on the endpoint, which is **LBI**. This approach was championed by a vendor called Bromium.

Initially, LBI had significant limitations, because:

- It was quite compute-intensive, taking CPU cycles away from the enterprise apps the user was working in.
- 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.

Figure 5: Local browser isolation: doing the isolation on the endpoint



Source: Omdia

Bromium worked to improve matters regarding the first issue, i.e. the compute overhead. However, with regard to the second it could be argued that Bromium was simply ahead of its time in that as laptop estates evolved, an increasing proportion of them would be based on newer silicon and thus would support LBI. In any case, the vendor was ultimately acquired by lap- and desktop manufacturer HP in September 2019.

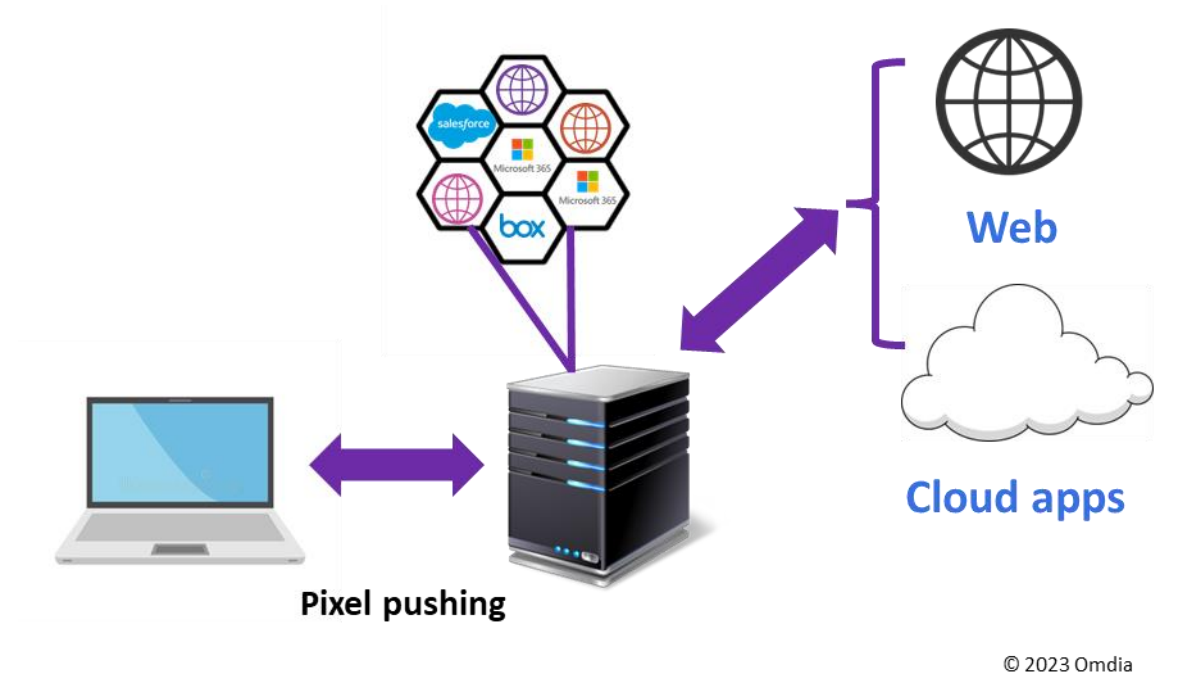
Remote browser isolation (RBI)

The other approach, RBI, performs the same function, i.e. isolating the session within a VM on a server and presenting a sanitized version of the webpage to the endpoint. This approach was more popular due to the shortcomings of LBI outlined above. Several RBI vendors emerged, and a number of them were acquired by larger cyber firms that wanted to broaden their portfolios.

The best-known dedicated RBI vendor still in existence is Menlo Security. Symantec, now part of Broadcom, also offers an RBI capability thanks to its 2017 acquisition of RBI start-up Fireglass. There

are a range of other vendors in this part of the market, including Ericom and Apozy, though the latter's technical approach, called native browser isolation, is slightly different to traditional RBI.

Figure 6: Remote browser isolation: doing the isolation on a server and pushing pixels



Source: Omdia

Remote browser isolation is primarily delivered as a service by a third-party provider, although some enterprises run it themselves on a separate server attached to the corporate network. When a user requests a webpage, whether via their desktop or mobile browser, the service creates an isolated browser session in a disposable containerized instance. The page is presented on the browser as a rendering, commonly as pixels over an HTML5 canvas.

Keyboard and mouse inputs are transmitted to the isolation service via an encrypted channel, and any resulting updates to the remote browser webpage are sent back to the endpoint device in the same way. Because no active content is downloaded, any hidden malware or viruses in the page are unable to reach the endpoint.

While it is clearly superior to the local isolation approach, RBI is not without its drawbacks. It is bandwidth-hungry at least if it is to deliver a satisfactory user experience. Furthermore, since pixel-pushing is resource intensive, RBI services tend to be expensive. There can also be issues around scalability, depending on the architecture of the company providing the service.

Making changes to the browser instead of isolating it

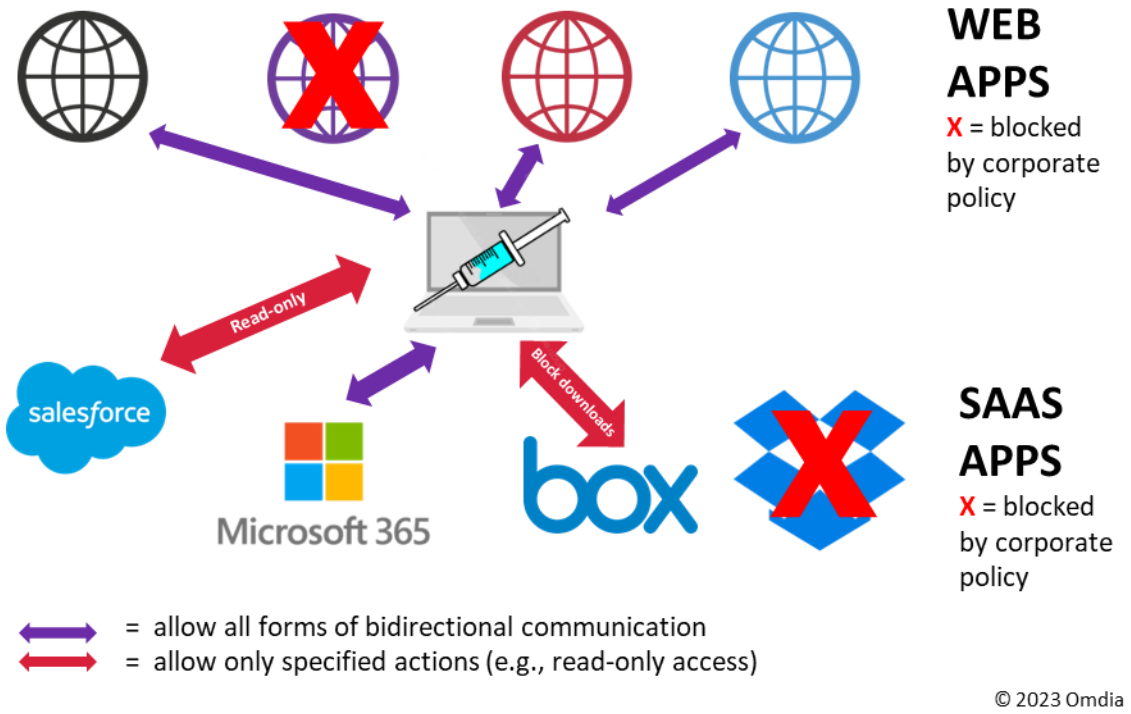
More recently, the focus has shifted to making changes to the actual browser instead of isolating it. In other words, instead of putting each browser session into an isolated environment—along the lines of a DMZ so no harm can come to the underlying infrastructure—the idea now is to empower the browser itself to avoid any problematic browsing activity. Where browser isolation was like a "controlled explosion," the new approach engages in the policy-driven blocking of anything explosive.

Here again, two distinct approaches have emerged.

Browser extensions

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.

Figure 7: Browser extension: injecting JavaScript to enforce security policy



Source: Omdia

Developing a browser extension involves somewhat less work than creating a brand-new browser, even if the latter task is now facilitated by the preexistence of the Chromium framework (see the following section on enterprise browsers). Indeed, there are extensions in the thousands (see the section above on plug-ins/extensions) created for many different purposes, including user interface modifications, cookie management, ad blocking, and the custom scripting and styling of webpages. Security is just one more use case, and there are multiple vendors offering security-specific extensions including Seraphic Security, LayerX, and Xayn.

Proponents of the extension route argue that it is a less-disruptive approach to browser security than a dedicated "corporate" (i.e., enterprise) browser, even though the latter does not necessarily require a complete rip-and-replace operation. Clearly, in as much as it is only an extension to the existing consumer browsers that ship with a laptop or other mobile device, it should prove both a simpler deployment and, potentially, a cheaper proposition overall.

However, its critics argue that it is an experimental approach, in that it operates after the content has been rendered, its only option therefore being to block that content. In addition, and more seriously from an operational standpoint, they point to the fact that Google is significantly changing the upcoming Version 3 of its Manifest API, which governs how Chrome extensions interact with the browser.

Given the proliferation of malicious content in apparently harmless extensions, the rules are to be tightened considerably to the point where many extensions simply will not be able to operate. This could make life more difficult for the browser extension camp as a whole, if not render its technology outright inoperable.

Enterprise browsers

The second approach is the development of a completely new browser, for use whenever an employee is accessing the internet or cloud apps for work.

The basis for all these enterprise browsers, as they have become known, is the open-source Chromium project, developed and maintained by Google. To the base Chromium, enterprise browsers add security-specific features such as integration with a customer's identity provider (IdP), such as Okta or Azure AD, as well as with their provider of single sign-on (SSO) services.

These integrations enable enterprise browsers, in the scenario where they are coexisting with a standard consumer browser on an endpoint, to block access to any corporate applications, whether SaaS or web apps, from the regular browser and thereby enforce the use of the secure browser for that purpose.

An enterprise browser thus comes with all the security policies required for protecting an organization, such as completely blocking access to dangerous or inappropriate sites, as well as imposing limitations on access rights. For instance, this may mean allowing certain users to read what's in their company's Salesforce instance but not copy, forward, or even download any of the information. Enterprise browsers also come with the ability to analyze incoming data, such as content a user is downloading from a sanctioned website, to see whether the content itself has anything malicious within it because the site has been compromised since last it was accessed.

Particularly significant, of course, is the fact that enterprise browsers do not require the complete replacement of the regular "consumer browsers" that ship with laptops and other mobile devices as

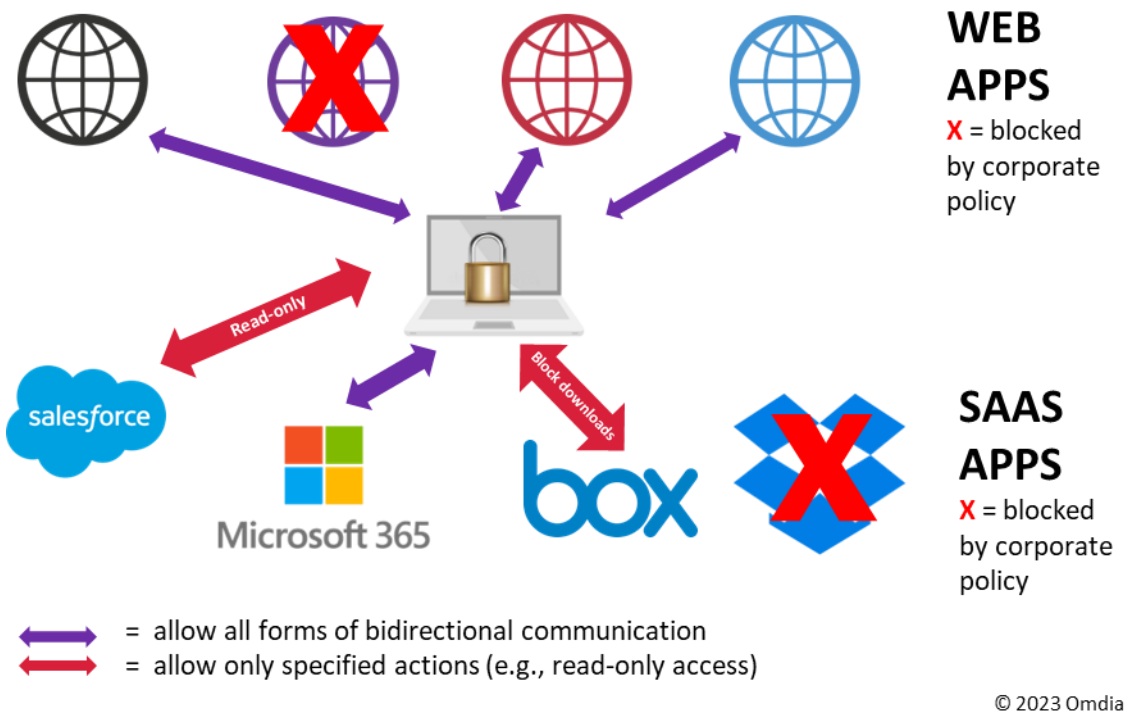
default. They can live alongside the standard one on the endpoint and be used for all corporate activity, leaving the other one for the user's personal browsing.

Suitability for BYOD

Coexistence is a key benefit in terms of the adoptability of enterprise browsers, particularly for companies that have a BYOD policy for endpoints or have a lot of contractors working for them on a temporary basis. For more risk-intolerant companies, meanwhile, the enterprise browser can, of course, completely replace its consumer counterpart and be used for all the browsing from that machine.

To clarify: the option of coexistence does not imply a way for rogue users to circumvent the enterprise browser's use. This can be mandated programmatically thanks to the integration with an IdP, with a pop-up advising the user that they can only use the enterprise browser to access a particular site. Furthermore, if they have sessions open with both the browsers on their device, data can be greyed out if they try to copy and paste it from the secure to the insecure environment.

Figure 8: Enterprise browsers: using a dedicated browser to enforce policy on corporate usage



Source: Omdia

Enterprise browser vendors were the object of considerable interest on the part of venture capitalists over the last couple of years. The two best-known participants in this market, not least

because they were chronologically the first and second entrants, are Island and Talon, both Israel-based companies, and they have raised $285m and $143m respectively in funding. A third still-more-recent entrant into this market is Surf Security, which is UK-based although both its founders hail from Israel. It has raised a more modest $26m but has only been in existence for a year.

However, other vendors also use the enterprise browser term. Citrix, for instance, in 2022 changed the name of the browser technology within its Citrix Workspace product, a virtual desktop infrastructure (VDI) platform, from Citrix Workspace Browser to Citrix Enterprise Browser, thereby associating it with the growing buzz around this technology area. However, that product is specifically for use with the vendor's VDI, so not really a standalone offering. In addition, Citrix has maintained a somewhat more muted presence in the market since its acquisition by private equity in September last year.

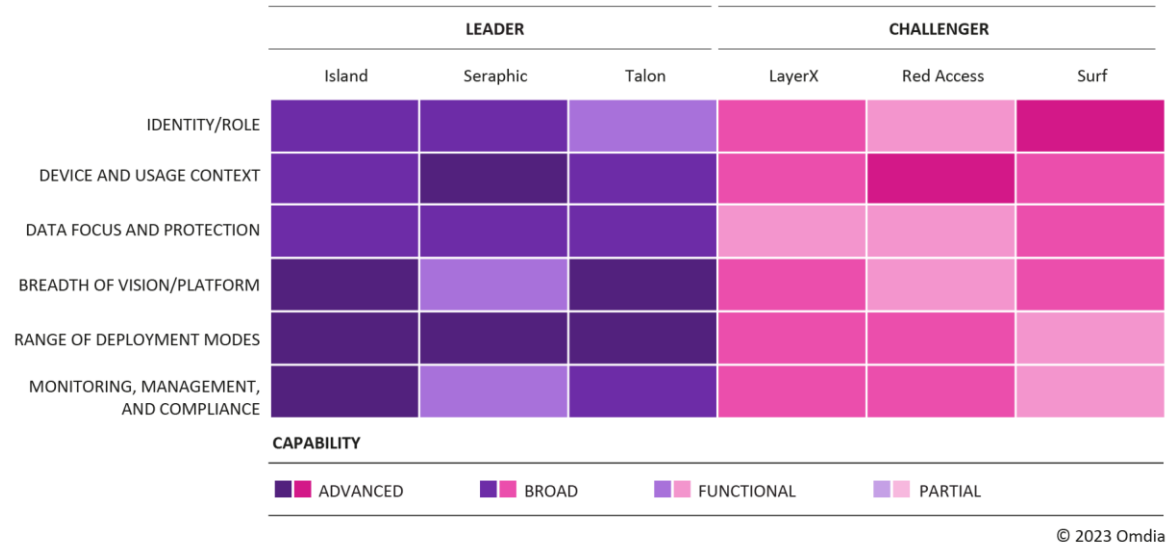
A smaller specialist vendor, Zebra Technologies, offers an enterprise browser specifically for use in industrial environments, such as on tablet devices mounted on forklift trucks.

Vendor landscape

Profiled players

In compiling this report, Omdia has spoken to and surveyed vendors across the three categories of browser security, i.e. RBI, browser extensions, and enterprise browsers. As will be clear from reading the vendor profiles that follow, some of them offer hybrid platforms (e.g. Red Access and Talon). The focus for the report has been on companies that are still primarily or exclusively vendors of browser security technology, whether in the browser extension or enterprise browser category.

Figure 9: Omdia Market Radar on Browser Security, 2023



Source: Omdia

That said, we do include some level of information on companies such as Menlo Security, which has expanded its remit well beyond RBI and can no longer be said to live or die on the strength of its browser security technology alone. We include a profile of Menlo given its importance as the flagbearer for RBI, but without subjecting it to the comparative process. There are also profiles of three other RBI vendors: Authentic8, Ericom (now part of Cradlepoint), and Garrison, although again they are not part of our comparison.

SSE and SASE take RBI mainstream

We also refer to the growing trend for broad-based network security vendors that were already bundling various capabilities such as firewall, secure web gateway (SWG), zero trust access (ZTA),

cloud access security broker (CASB), and data loss prevention (DLP) into cloud-based proxy offerings (SSE and SASE) to add RBI into the mix. What this trend shows overall is that while it did not become a major market segment in its own right, RBI technology remains relevant and, if anything, has gained greater importance in the current environment of cloud-first infrastructure and hybrid work.

However, we have not included those SSE or SASE vendors in the comparison of browser security capabilities, because as "security generalists" they compete at a different level from the pureplays on which we focus here. Nonetheless, they must be remembered as competitors for the corporate budget that the specialists are going for, arguing that RBI can be an extra tick-box item. The specialists, meanwhile, must convince potential customers that it is worth devoting part of their budget specifically for browser security, rather than buying it as part of their SSE or SASE: it is the eternal dichotomy of the specialty store versus the supermarket.

The rankings

Concerning the rankings attributed to the vendors we have compared in this report, we should point out that all the scores were very close, making the overall competition here a close-run thing. A point either way could have pushed a Challenger into the Leader category or a Leader down to Challenger status. That said, it is worth describing our thinking in rating and ranking the vendors.

Island

Island is a Leader for various reasons. Firstly, because it was essentially the creator of the enterprise browser category, coming up with the description of the product class and successfully imposing it on the market as a whole, even though the analyst house that traditionally names emerging segments decided, in adopting the term, to muddy the waters by applying it to both dedicated browsers and extensions.

Secondly, Island attracted a considerable sum of VC money, which has enabled it not only to pursue its technology roadmap but also to engage in the kind of evangelical marketing required to establish an emerging technology in the broader landscape of cyber.

Thirdly, we like the vendor's vision for its future of becoming a platform not just for security, but multiple other use cases for its customers.

The Challengers

As mentioned above, our three Challengers all scored well and could very easily have moved into the Leader segment. Often they were at a slightly earlier stage in the development of the product and/or go-to-market strategy. In some cases, they have raised less funding to date, thus limiting their ability to elevate their profile in the market for the time being.

Notwithstanding, some aspects of their platforms were interesting and, in some cases, even market-leading in our opinion. However, overall their offerings were just not as comprehensive at the moment.

Now, let us profile a handful of other vendors who are not part of the comparative process for this report, but which are worth putting on your radar when you are considering your options for browser security.

Vendors in the market radar for browser security

Island

The days when apps lived on users' desktops, laptops, or 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 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 at the forefront of efforts to address it and is well positioned to gain significant share in the 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 being lumped into a "secure browser" market, casting itself instead as a broader player with a platform that enables security plus other benefits with the use of its browser.

The Island Enterprise Browser can replace the standard browser on a user's laptop or 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 compared with conventional browsers.

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

Product 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 desktop 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: that provided by the open-source Chromium project developed and maintained by Google. It then added in its own features, which include integration

with the customer's identity provider such as Okta or Azure AD as well as with their provider of single sign-on (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 it has 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 versus coexistence

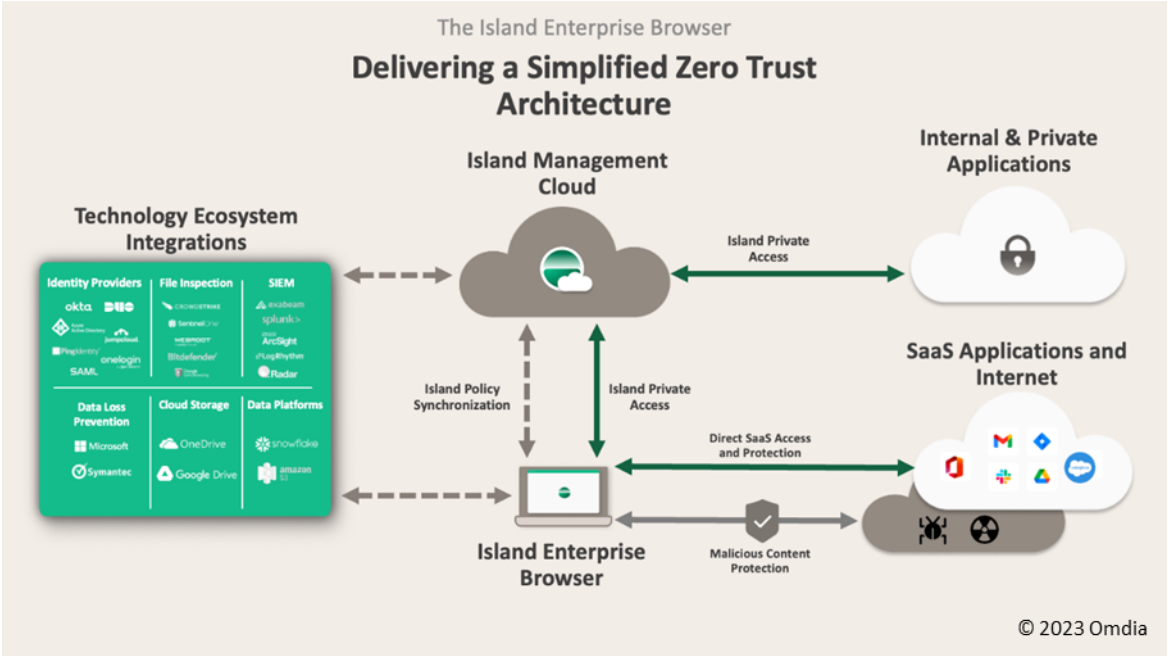
Island refers to the scenario in which its browser replaces standard Chrome, Edge, or Safari on the endpoint as the full browser use case, which is favored by the most security-sensitive organizations. The other, more common one is where it lives alongside the standard browsers and any engagement with 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, the 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 log-in credential secret from the user, who is logged in once they have filled out the appropriate pop-up information.

Greying out sensitive data

Island has also 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 greyed 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.

Figure 10: The Island Enterprise Browser



Source: Island

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; before that, he was GM and CTO of McAfee. Meanwhile Amiga was founder at CTO of Fireglass, a RBI company also acquired by Symantec in 2017. He was also a founding investor at various companies, including SSE vendor Axis Security, Build Security, which offered a permissions policy management platform for developers and was 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 downmarket (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 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.

Meanwhile, in January 2023 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. However, as the first out of the gate in the last category, Island feels it has a lead over the other vendors in the space, while against 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, 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 particular 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

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 2020
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

Appendix

Further reading

Cloud Services End-User Survey – 2023 (June 2023)

AT&T and Cisco partner to provide better hybrid working experiences: Exploring the broader context of business mobile convergence (BMC) (June 2023)

On the Radar: Red Access injects security into browsing (June 2023)

Developments in Browser Security: From Isolation to Enterprise Browsers (March 2023)

On the Radar: Surf offers zero trust via its enterprise browser (March 2023)

On the Radar: Talon offers endpoint and web security with an enterprise browser (March 2023)

On the Radar: Island offers an enterprise browser for security and productivity gains (February 2023)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

Rob Bamforth, Associate 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

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are

subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

askananalyst@omdia.com