Secure Enterprise Browser (SEB)

The Newcomer to Cybersecurity

Speaker: Brian Kenyon, Chief Strategy Officer, Island
Moderator: Sean Costigan, Professor, George C. Marshall European Center for Security Studies
Report Author: Hind Idrisse, Assistant Professor, National School of Applied Sciences, Khouribga

Introduction

Today, the digital transformation has totally reshaped both the way we work and the infrastructures enabling that work. This absolutely includes the way how enterprises deliver and access applications. With the proliferation of cloud-based services (basically SaaS solutions), and the rise of hybrid work with connected devices everywhere, businesses are moving even faster while operations are made more simple and efficient.

The browser is the foundational access point to the world of web applications and SaaS solutions, and the new workspace for modern business users. It is the application that enterprises use the most, and where employees spend most of their working hours, performing nearly all of their day-to-day responsibilities, from checking emails and filling sheets, to sharing files, developing processes and engaging customers, colleagues, and partners.

However, a browser is not an enterprise application. It has a little visibility and control over unmanaged and untrusted devices accessing the enterprise resources. This unfortunately exposes the business to a wide range of cyberattacks and data breaches given that nowadays most contractors, vendors, partners and home-based employees frequently access enterprise apps and systems via their own endpoints.

What is needed is a browser specifically designed for the enterprise and embedded with robust and flexible security functionalities to help defending against malicious attacks and data theft. Verifying and validating non-corporate devices before granting access to the system and related data is at the top of security features to be considered and implemented.

Island, the world's first enterprise browser, is the workspace of the future enabling organizations to protect users and data without compromising simplicity and fluidity of workflows. This paper describes what a secure enterprise browser is, why it is required, and what makes it such successful.

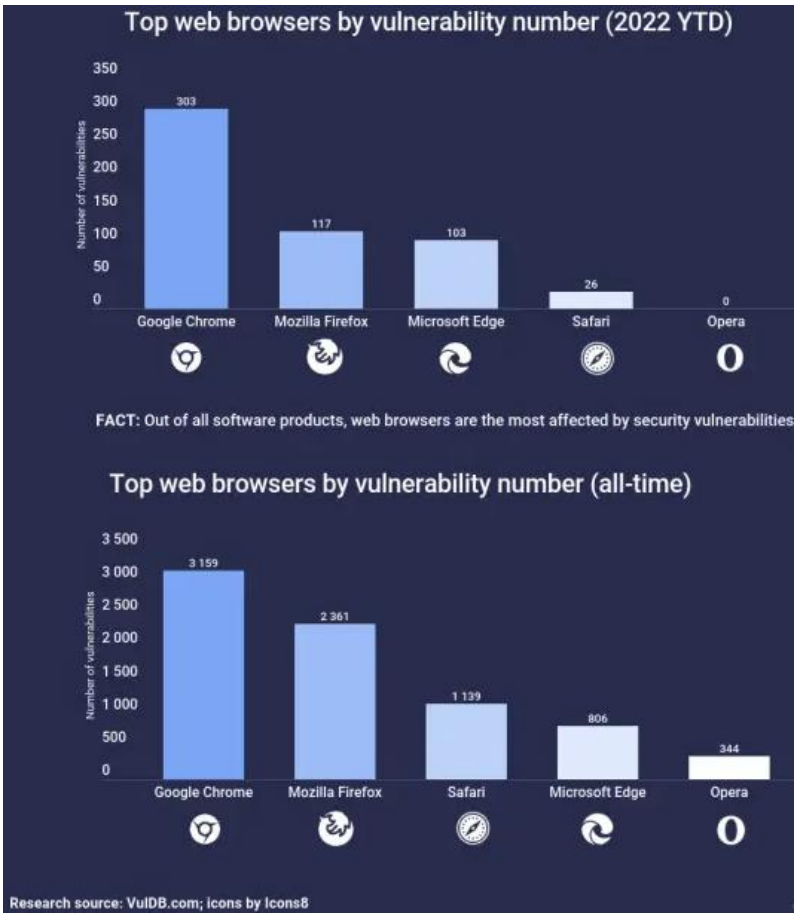
Why a Secure Enterprise Browser?

Hackers are targeting businesses more than ever before. Currently, most enterprises create and implement line-of-business services in public clouds, and employees now use browsers for much more than simply web browsing. Moreover, in the post-COVID era, the world witnesses a dramatic increase in the adoption of hybrid work and use of SaaS and internal web apps, allowing access from home and office using both company-owned and employee-owned devices. On one hand, this truly help managing and alleviating the workload since browsers encompass all facilities employees need for almost all their daily tasks. But, on the other hand, this increasingly makes browsers a popular target for adversaries.

Hackers frequently take advantage from consumer-browser vulnerabilities to penetrate systems, steal sensitive data and cause damage. They can easily install ransomware or inject any other type of malware that help remotely conducting attacks.

Furthermore, free browsers like Chrome, which are fundamentally conceived to gather user data and earn money from advertising, are easy prey for attackers basically due to their tracking capabilities and poorly secure plugins policies. Google published in March 2022 a blog post reporting a spectacular rise in high-severity threats affecting Chrome and other Chromium-based browsers like Microsoft Edge and Brave.

In addition to degrading the vital-business IT system and causing considerable financial losses, such cyberattacks and data breaches heavily harm the enterprise's reputation and may result in high compliance penalties and recovery costs.



Virtual private networks (VPN), remote browser isolation (RBI), and virtual desktop infrastructure (VDI), are among popular solutions adopted by enterprises to protect remote workers against threats originated from browsing over Internet. However, the majority of these technologies are found inappropriate for Cloud Apps and Web Services as they introduce conflicts in security restrictions, degrade performance and usability, and reduce user satisfaction.

What is a Secure Enterprise Browser?

Given the emergence of web browsers as the entryway to the web, and thus to work, it has become mission-critical for dedicated security solutions to defend against attacks and data loss, alleviate privacy concerns and boost users trust.

A Secure Enterprise Browser (SEB) is a browser specifically designed for the enterprise. It is built with cutting-edge security functionalities to control how the browser behaves and deliver the ideal work experience to users while maintaining the core security of work itself.

Island, the leader and pioneer in the Enterprise Browser market, released its award-winning enterprise browser with not only basic security controls and governance features, but also with a range of customizable productivity and user experience enhancements. In other words, Island browser gives organizations complete control, visibility, and governance, while providing consumers with the same fluid Chromium-based browser experience they expect.

Island is primarily engineered to protect against zero-day exploits and other vulnerabilities. It ensures compliance of endpoints with corporate standards, and blocks browser manipulation or any other malicious behavior basing its anti-tampering capabilities. It also advocates for rules and policies to protect user privacy given that it does not fully control of the user's device or obtain access to the user's personal applications or data.

Finally, secure enterprise browsers are the perfect solution to extend corporate web apps and services to unmanaged and untrusted devices, as well as to overcome the fundamental performance, cost, and UX constraints of conventional VPN, VDI, and RBI solutions.

Key Use Cases

The Island Enterprise Browser is used across all industries, including healthcare, financial services, manufacturing, retail, aviation, and technology.

A growing number of unprecedented enterprise use cases are now made possible by the use of Island Enterprise Browser. This includes governing and securing critical SaaS and internal web applications from data leakage, ensuring safe access and fluid work for contractors and BYOD workers through setting granular policies, and keeping full governance over privileged user accounts by monitoring and capturing all critical enterprise activity.

Island also delivers a native and pleasant user experience for the hybrid workers in contrast to the costly and ineffective virtual desktop infrastructure (VDI), while supporting built-in safe browsing, web filtering, web isolation, exploit prevention, and Zero Trust network access at much lower cost.

Conclusion

Although SaaS solutions and web applications are reshaping the workplace, they are also creating new opportunities for threat actors and new challenges for corporate IT and security teams. With improved visibility, control and productivity, secure enterprise browsers are designed in view to alleviate security and privacy concerns that arise with the proliferation of hybrid workforces, unmanaged devices, and web services. Island is the world's first enterprise browser specifically created with a comprehensive set of cutting-edge embedded security capabilities, while also ensuring lower complexity and cost.