InformationWeek

WEBINAR SUMMARY

March, 16, 2022

Why Browsers Need to be a Strategic Application

Brian Kenyon, Chief Strategy Officer, Island Technology
Joseph Blankenship, VP & Research Director, Forrester

KEY TAKEAWAYS

- Browsers play an essential role in today's business operations, but security is a growing concern.
- Island Technology has changed the game by creating a user-friendly, secure enterprise browser.
- Island's enterprise browser integrates closely with enterprise security tools.
- No matter where employees are working, Island supports a consistent user experience and security policy.
- An enterprise browser addresses persistent security challenges like complexity and the changing threat environment.
- Last mile control revolutionizes the way organizations approach application security.

in partnership with

Island

OVERVIEW

The browser is the critical point where employees, enterprise applications, and underlying data meet. It's the world's most widely used application, but browser designers have ignored the needs of the enterprise. Island Technology has broken this paradigm with its secure and user friendly enterprise browser. Companies now see the value of implementing enterprise browsers to address specific use cases like critical SaaS protection, contractor access, and hybrid worker protection.

CONTEXT

Brian Kenyon and Joseph Blankenship explored challenges facing chief information security officers and discussed how the world's first enterprise browser is addressing their issues.

KEY TAKEAWAYS

Browsers play an essential role in today's business operations, but security is a growing concern.

Many business tasks have moved into the browser. However, every browser in use today was built with a consumer mindset to drive ads, search, and web-based collaboration. Popular browsers like Chrome, Edge, Safari, and Firefox aren't optimized for the security needs of the enterprise.

Historically, IT teams have used network-based security controls to bolster web application security. These tools, however, are losing efficacy due to increased cipher strength and changes in protocols like the shift from TLS 1.2 to TLS 1.3. Even SaaS providers' terms of service now stipulate that it's an infringement on the maintenance and support agreement if you break and inspect the web traffic before it gets to the provider or application. Another long-standing security remedy has been browser extensions. However, browser manufacturers have been shrinking the extension space and privileges due to malicious activity in that area.

Enterprises need a new approach to secure users and their browser interactions. A promising option is reinventing the web browser itself to provide a consistent, secure browsing experience. This can deliver a major positive impact, without requiring a massive security stack.

> Browsers have become more prolific and heavily used in our agent infrastructure, but we're losing the ability to impact security inside the browser. At a high level, it's almost like a new OS that we've been given.
>
> *Brian Kenyon, Island Technology*

Island Technology has changed the game by creating a user-friendly, secure enterprise browser.

Like other major browser companies, Island Technology built its enterprise browser using the open source package called Chromium. As a result, the end user experience is identical to what employees have become accustomed to in their browser of choice.

Historically, security has impeded users' web browsing experience and created friction as employees try to complete their work. Downloading files, for example, can be very slow due to security analysis in the background. Island's enterprise browser is unique because it focuses on the user experience first.

Island brings the control point very close to users, in the applications they are using. It's possible to create custom messages in Island that speak directly to users. Being close to the user matters because almost every application installed on local endpoints has a mechanism to exfiltrate data. With Island, it's impossible for users to pull data out of an application if the enterprise has classified it as sensitive.

> Tying security directly to the user interface has been an epiphany for Island. It has changed the way the company builds and deliver solutions, as well as how it communicates and works with the end user.
>
> *Brian Kenyon, Island Technology*

Island's enterprise browser integrates closely with enterprise security tools.

Brian Kenyon described how Island's enterprise browser works hand in hand with existing enterprise security systems:

- **Directory services integration.** When users open the Island enterprise browser, it authenticates them with directory services. This identifies who users are and what they are allowed to do.
- **Security operations center (SOC) integration.** Island monitors and creates a log of all user activity during a browsing session. Companies can build policies to determine how granular auditing should be. All information is fed back to the SOC.
- **Analytics platform integration.** Data from Island is enriched so organizations have context for security investigations.
- **Enterprise malware inspection and data loss prevention toolset integration.** The Island browser waits for validation from other security tools before allowing uploads, downloads, or file operations like save or print. A policy engine dictates what users can do and gives organizations a level of last mile control over the user environment which has been lost in recent years.

No matter where employees are working, Island supports a consistent user experience and security policy.

Historically, it's been difficult for companies to support consistent security policy control and a consistent user experience for all workers. Island's enterprise browser addresses these challenges. It's a universal application that can be used with managed and unmanaged devices.

IT teams can give Island to third party contractors or employees who want to connect on vacation from their own devices. The enterprise browser includes device posture capabilities similar to mobile device management (MDM) tools. Island checks each device and if it has basic security controls in place, users can access enterprise applications. Island's enterprise browser is a safe, governed medium that enables organizations to be very flexible in where, how, and when they allow users interact with applications.

During the COVID-19 pandemic, one of Island's early customers transitioned a large call center to remote work. Remote employees authenticated to the Island enterprise browser and the company took advantage of the native controls in the browser that mirror a virtual desktop infrastructure (VDI) environment. The company could see everything that remote workers were doing. In addition, the browser made it possible to redact data, prevent copy and paste, prevent screen captures, and watermark data to stop employees from taking pictures of their screens with a phone camera.

> Historically, consistency of experience and consistency of policy have been very hard to do. This is especially true with remote and hybrid office scenarios. Part of the solution is having consistent policy control no matter where an employee is.
>
> *Joseph Blankenship, Forrester*

An enterprise browser addresses persistent security challenges like complexity and the changing threat environment.

Each year, Forrester conducts a security survey. Major concerns facing security leaders include the complexity of the IT environment and the evolving threat landscape.

Island's enterprise browser reduces complexity by making it easier to instrument applications for security and easier for end users to work in a secure manner. After employees log into the browser, the company policy downloads and then they have instant access to all their web applications. Island makes it possible to work from an untrusted device in a safe and governed way.

Complexity is also the enemy when it comes to the changing threat environment. The more complex the security architecture is, the more difficult it is for IT teams to obtain actionable intelligence around real risks and transform it into a security plan and security controls. Island's enterprise browser provides a simple implementation of intelligence to get to an actionable result. The browser can immediately block access to particular sites, binaries, or executables.

> When it comes to malicious insiders, I could see the potential for a browser-based security approach which would be more eloquent than our current mix of controls.
>
> *Joseph Blankenship, Forrester*

Last mile control revolutionizes the way organizations approach application security.

Last mile control focuses on two areas: how the browser works and what users can do inside the browser in a given application. When network-based controls are used to secure browsers, it's impossible to prevent users from copying or printing. In contrast, last mile control like Island's enterprise browser stands between the user, key board, and device.

IT teams have great flexibility when deploying Island's enterprise browser. It can serve as the primary browser for the organization or it can sit next to other browsers. For example, organizations may require Island's enterprise browser for certain users or to access certain applications.

BIOGRAPHIES

Brian Kenyon

Chief Strategy Officer, Island Technology

Brian Kenyon drives corporate strategy at Island as its Chief Strategy Officer and one of the company's founding members. Brian has also held the role of CSO at Symantec and Blue Coat Systems. He built his early career in technical roles for more than a decade at McAfee where he was Chief Technical Strategist, as well as CTO, and served as chief architect at start-up Foundstone.

Brian is the author of *Security Battleground: An Executive Field Manual*; *Security Sage: Guide to Hardening the Network Infrastructure*; and *Special Ops: Host and Network Security*. He holds a B.A. degree in Finance from Loyola Marymount University.

Joseph Blankenship

VP & Research Director, Forrester

Joseph supports security and risk professionals, helping clients develop security strategies and make informed decisions to protect against risk. He covers security infrastructure and operations, including tools for the security operations center (SOC) such as security information and event management (SIEM), security analytics, and security automation and orchestration (SAO). He also covers security topics like artificial intelligence (AI) for cybersecurity, email security, distributed denial of service (DDoS), and network security. His research focuses on security monitoring, threat detection, insider threat, phishing prevention, operations, and management.

Joseph has presented at industry events, been quoted in the media, and written on a variety of security topics.