Enterprise Browser Management – The Last Mile Challenge

Reimagining the role of the browser in the enterprise security architecture

By Brian Kenyon
Chief Strategy Officer

If you're an employee, it's never been easier to be productive. Cloud computing and modern collaboration tools allow us to work almost anytime, anywhere. Being a hybrid worker is now the norm, rather than the exception.

If you're tasked with securing a workplace, however, this flexibility comes with unique challenges. Reliance on BYOD, the cloud, virtual desktops and remote work accelerated dramatically during the pandemic. The result, cybersecurity professionals are now contending with a different set of cybersecurity challenges around protecting their critical resources.

Security concepts such as Zero Trust – and the usual array of data loss prevention, identity management and cloud access security tools – offer a framework for managing risk. Until now, a major component of this stack has been omitted yet there is also a glaring omission from this approach: the web browser.

The Limitations of the Consumer-Focused Web Browser

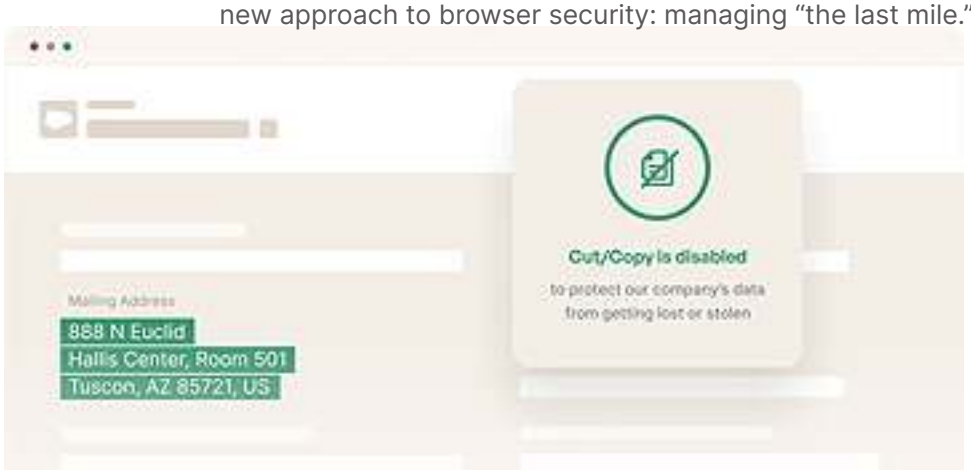
Many of the productivity tools we use are not purpose-built for enterprise security. The web browser falls squarely within this category. Consumer-oriented browsers are especially vulnerable to insider attacks, as organizations often have little control over what users do while interacting with applications and services within their browsers. Compounding the problem, they also often lack visibility or an ability to review prior user activity at the last mile.

Different users require different levels of permissions based on role or function, and businesses are quite familiar building policies to support this for the network, OS, and application layers. By assigning privileges based on whether you're a user, a manager or an admin, organizations can exert a bit more control over the roles of users to determine what they can and cannot do, per application.

Making matters worse, standard consumer web browsers pass this traffic, but have little role to play in enterprise interactions. Instead, today's browsers are designed to provide a seamless user experience that helps monetize consumers through advertising, tracking and search optimization. They are not designed for enterprise-grade security.

Which is unfortunate because browsers are also deeply embedded in almost everything businesses do. The productivity applications and SaaS platforms that organizations rely on are heavily browser dependent.

As a result, businesses are taking immense risks in how browsers are being used today. But what if we reimagined the role of the browser in the enterprise and delivered a new approach to browser security: managing "the last mile."



The enterprise browser must give control over how users interact with information, particularly cut, copy, paste, download, upload, print, and screenshot based on corporate policies.

Island

Why Managing The Last Mile is the Key to Minimizing Risk from Browsers

In simple terms, the last mile is a security concept that defines where employees, applications and the data moving through those applications meet within the critical last mile of the browser. This critical intersection happens in the browser yet is often overlooked, with security efforts largely being focused on controls in the network and in the operating system.

So why, if the last mile is truly so important, has it gone unaddressed for so long? The answer is simple: Major browsers such as Chrome and Edge are not built for the enterprise and thus lack last mile control. This means businesses have not been able to adequately prevent application misuse and malicious activity occurring within browsers.

Currently, organizations must take a sledgehammer approach to managing such situations. One example: They may ban all use of private Gmail accounts via a proxy rule. This approach restricts productive workers and creates inefficiencies, however. Rather than taking a sledgehammer to the problem, organizations can now wield a scalpel – in this case by applying last mile control over the mail client., For example, the policy can allow Gmail but prevent interactions such as file uploads or pasting of data to personal Gmail.

A Closer Look at How Last Mile Control Works

Consumer-grade browsers do not offer a way to implement last mile security policies and are not built with enterprise security as the focus. As a result, they uncontrollably leak (or truly gush) data down to the endpoint. Additionally, when data is on a user's screen, it is no longer encrypted and is vulnerable to misuse. Screen captures, print outs, downloads, copying and pasting into a personal application, or even a user taking a smartphone photo, are some of the risks to consider.

An enterprise browser allows organizations to manage these risks by incorporating a centralized management console for policy enforcement. This added layer allows for the setting of policies that govern activities such as downloading, saving, cutting-and-pasting or screen grabs within critical applications or to destinations that may be less than desirable.

Context is one critical aspect of last mile control. For example, taking the sledgehammer approach and banning all cut-and-paste browser activity across an organization would quickly create a fiasco in many cases. Yet a browser designed to allow control of such actions should have great flexibility as well to ensure that employees can perform such actions as cut-and-paste across key SaaS or internal web applications without the risk of data leaving the work environment. This is simply one of many types of last mile control options that are opened up with an Enterprise Browser. Ensuring that employees can work naturally in this way offers a far more precise and less disruptive solution.

Can a Last Mile Browser Operate Efficiently?

You're probably thinking that such precision is great – but is it scalable? How do you manage assigning many different controls based on environment, context and the users involved?

The truth is that the practice of role-based access is already ingrained in today's organizations. An enterprise, last mile-focused browser simply adds an additional layer providing governance in areas that have always been out of reach. Given how radically it can improve bottom-line security (remember, current browsers are often a complete cybersecurity blind spot) the ROI is heavily in its favor.

A true enterprise browser can also help reduce resource usage. Let's consider one common scenario: A company has several internal applications that are vital to their operations, yet they are older and insecure. Attempting to address this problem by inserting new security controls or governance is often tedious, expensive, and potentially disruptive.

Instead, a company can improve security more efficiently by addressing it at the last mile by using a browser that offers effective controls. A browser that offers the same UX as Chrome (or any other browser built on Chromium), but that also allows you to manage and control user behavior and access through the creation of simple policies and rules, is a much-needed innovation.

Other Key Features of an Enterprise Browser

A browser is situated in a unique position regarding the flow of information. This privileged perch makes it a powerful cooperative resource within a company's security architecture. An enterprise browser can take advantage of this in a variety of ways.

First, an Enterprise Browser can live peacefully alongside existing browsers. It does not have to be the only browser in use. However its use can be enforced anytime a user engages a critical application and gracefully transition the use over the Enterprise Browser at the time of need.

Enterprise Browser Enforcement ensures that all critical application engagements are governed while letting users have the freedom to use their alternate browsers for personal or non-critical business needs. Another important element of an enterprise browser is that it ties into the existing infrastructure of the organization using it. Before data is downloaded, uploaded or viewed, an enterprise browser can send it to a third-party security solution for inspection. This is simpler and more efficient than relying on costly network layer traffic redirections which require complex decryption.

Users will be comfortable with it because it looks and acts like the browsers they are accustomed to; organizations will feel equal comfort because it allows them to deal with familiar objects. such as users and groups in their directories, as they construct policies. In other words, it provides an identical user experience to consumer browsers, while governing the last mile.

In addition, an advanced enterprise browser can also audit user behavior in a way that has never been possible before. If someone is acting maliciously and trying to take a screen grab or copy data from a critical application area, the browser puts eyes on it. In the process it can create a complete audit record of those activities to be leveraged both within an administrative purview as well as to be fed to external SIEM security tooling such as Splunk. These are activities that generally reside entirely outside of cybersecurity tooling and protocols thus provide immense value and visibility like never before.

Users will be comfortable with it because it looks and acts like the browsers they are accustomed to; organizations will feel equal comfort because it allows them to deal with familiar objects.

It's time for a browser that plays as a cooperative resource in the enterprise security ecosystem.

Better Security by Doing Less and Saying Yes

You may wonder if adding greater control via the browser real-estate is necessarily better, especially in a world where flexibility and collaboration have become paramount. Yet the truth is that by adding a new level of control to a browser, a company is less restricted, not more. Suddenly, with new guardrails in place, it is possible to use consumer applications that were once off-limits. New ways of using applications suddenly become possible. The sledgehammer approach goes out the window, and only the restrictions that are truly necessary are now in place.

Last mile control isn't about stopping activity or mitigating threats; it's also about allowing organizations and users the freedom to be maximally flexible and collaborative while simultaneously improving security. Organizations improve security by doing less -- and improve morale by saying "yes" to things that were once off-limits.

The Takeaway

The expanding use of hybrid work, BYOD, virtual desktops; the need for contractors to access internal systems and increasing adoption of SaaS platforms and reliance on vendor security are just a few of the issues challenging organizations today.

Yet here's the good news: All these challenges can be met simultaneously by addressing them at the browser. By finally having the ability to manage the last mile, companies can streamline their security efforts, reduce the resources they must spend and profoundly lower the cybersecurity risks at the intersection where people and data meet.

The bottom line: It's time for a browser that plays as a cooperative resource in the enterprise security ecosystem and gives organizations true control over the last mile.

About Brian Kenyon

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 Foundstone.

About Island

At Island we are focused on delivering an enterprise browser that enables data protection, access controls and full logging and visibility into all interactions with web-based applications. Our Island Enterprise Browser is built on last mile controls that enforce policy over actions. Island is led by senior executives from the security and technology industry and backed by the world's leading venture funds -- Insights Partners, Sequoia, Cyberstarts, and Stripes. Based in Dallas with operations in Tel Aviv, Island can be reached via email at info@Island.io or (866) 832 7114.

Island