EDITORIAL BRIEF

Here's How to Solve the Data Leakage Problem from SaaS and Web Apps

Using an enterprise browser for data governance and protection

By Jason Trunk
Enterprise Architect, Island Technology

SaaS and web applications have exploded in popularity despite their weak governance around where critical company data ultimately end up. With the creation of the world's first Enterprise Browser, enterprises can now keep SaaS and critical web app information from leaking out to desktops, file systems, personal email, web conferences, external drives, even camera phones.

SaaS and internal Web applications have revolutionized how the modern workplace functions. The typically simple, seamless process of signing up and moving key business operations to the cloud has unlocked immense value and helped organizations avoid much of the heavy lifting they endured in the past.

As a result, organizations are adopting SaaS and Web apps in huge numbers. Unfortunately, this created a significant problem: It's almost impossible to maintain effective data protection and governance.

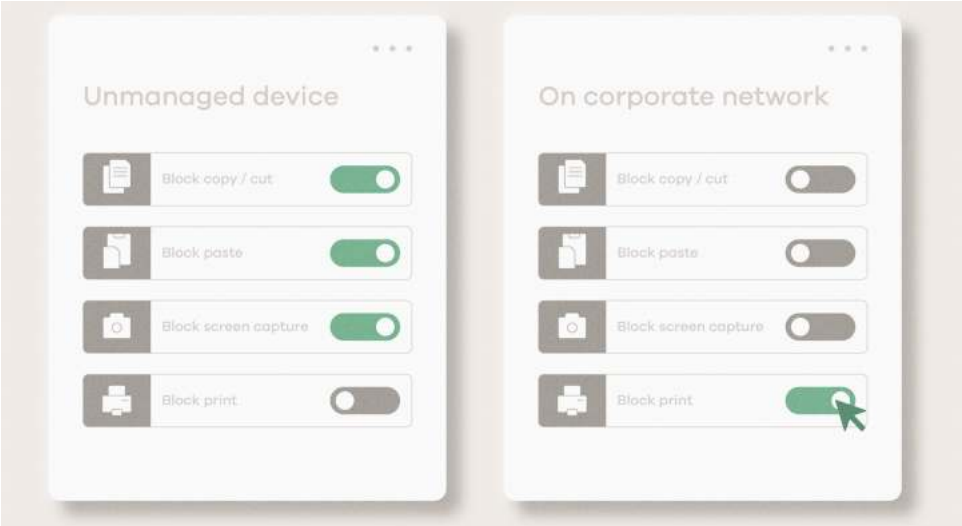
While the ease of using SaaS and internal Web applications is undeniable (just grab a credit card and you're ready to go in minutes), questions of security, legality, process, ownership etc. often fall by the wayside. When organizations have thousands of apps (sanctioned and unsanctioned) and departments and workers with varying needs and requirements, governance is a mess. In fact, it's more than a mess: It's an ongoing nightmare for IT departments. Growth in cloud apps is exponential, and governance has become absurdly complex. The need for constant exceptions (with different departments needing access to different things) has created a boondoggle of epic proportions. These exceptions add layers of complexity and degrade the security posture.

Why Have Prior Approaches Failed?

The historical approach for managing application risk involved things such as Web gateways and Cloud Access Security Brokers. However, gateways are built around broad categorization and lack fine-grained control over what you can do within an app.

Cloud Access Security Brokers offer more control but are very limited by the capabilities of the cloud provider. Using these tools is so cumbersome and ineffective that finding a better way of doing things has become a never-ending chase.

Fortunately, an elegantly simple solution has arrived: The creation of the first true enterprise browser.



An enterprise browser limits the risk of data loss in critical applications by creating a closed loop where nothing can pour out of the browser.

Island

Today when engaging with critical SaaS applications most organizations use consumer browsers such as Chrome or Edge. While consumer-based browsers are beautiful pieces of technology, they are not built with governance in mind. They allow users to log-in into applications and do things like copy and paste or print things shown on the screen. They provide no data governance in terms of user/app engagement --no control over what users can and can't do with an application.

Given this long standing browser governance problem, the industry has bolted on ineffective external technologies (data loss prevention, gateways, cloud access security brokers) to try and exert control.

Yet isn't it smarter to have the browser itself assert control? This is the genesis of the enterprise browser.

How an Enterprise Browser Solves the Problem

While role-based access controls associated with some applications can provide a degree of protection, they do not cover all the bases. One example: If a salesperson is logging in from a machine at their home through a critical SaaS app, that's still a dangerous proposition if that salesperson is exporting, downloading, or copying critical customer information from the screen. Sometimes even privileged users have access that should be governed. Asserting control at the right time, over the right app, for the right user, at a granular level, is the absolute key to good governance.

The process works like this: When a user logs-in using their single sign-on, an enterprise browser can check the device posture to ensure the user is originating from a trusted device when accessing critical SaaS applications. Then, policies are implemented. Organizations can block things like printing screens, copy and paste, saving data from the screen, screen capturing and sharing information over things such as web conferencing tools like Teams and Zoom.

An enterprise browser can also identify critical areas of an application where an organization might want to redact sensitive data types that are sitting in that application using automation scripts. An enterprise browser can also provide deep audit logging to provide a forensic log for investigation of every action a specific user took.

In addition to the above, the enterprise browser should be able to encrypt cookies to protect application sessions from outside intrusions, create data storage policies to ensure all interactions are safe, assure privacy and offer integrated malware scanning for uploads and downloads.

Ultimately, an enterprise browser will help limit the risk of data loss in critical applications by creating a closed loop – which means nothing can pour out of the browser. By attacking this problem in this manner, you are not constrained by the limitations of either the internal application or the SaaS providers.

Other Key Benefits

Let's take a closer look at a few areas where an enterprise browser shines within this context of SaaS and Web apps:

Compliance

Adopting this approach helps with compliance, attesting that certain data has not been exposed. With data regulation changing at a national and multi-national level – and varying considerably by jurisdiction – it is critical to manage regulatory risk by exerting flexible but fine-grained control, especially when application developers are struggling to keep up.

Flexibility

Another factor supporting the need for an enterprise browser is that every app has different capabilities and organizations are at the mercy of the SaaS provider in terms of what they can do. There needs to be a better way to enforce policies more uniformly across all organizational real estate. An enterprise browser will enforce policy uniformly across this real estate, yet also be very flexible where necessary for a given app (if data needs to be redacted or an action needs to occur, or a particular device postured, or device situation needs to be enforced).

Speed

Just as it is hard (if not often impossible) to get SaaS apps to change to fit your security needs, it is difficult to track down internal app developers to make needed changes on corporate applications when the developers may not have seen the code in a year. Many of the developers responsible may no longer even work for the organization. Additionally, older apps may even pre-date modern layers of security governance and therefore have very little protection. By attacking the problem at the browser level, you can quickly introduce changes to govern all these applications and enforce modern security in one step.

Productivity

The COVID-19 pandemic, which made telecommuting the default for tens of millions of workers, underlined the challenges involved with trying to reach legacy apps from home. For telecommuters or contractors, enforcing use of the enterprise browser over critical apps ensure they are completely governed as if on a corporate device. This also frees the organization to reap the benefits of distributed work teams. Remote workers can now safely engage with applications because they have prevented them from downloading files from that application to an unmanaged device. They have prevented them from copying and pasting. Rather than being punitive, it increases productivity.

The Takeaway

SaaS and Web apps are powering the modern workplace and bringing enormous value in the process. By using an enterprise browser to solve the longstanding problem of data governance and protection, organizations not only lower their risk, they also unlock even more value from the applications on which they rely.

About Jason Trunk

Jason Trunk serves as Enterprise Architect and blog contributor at Island with over 20 years of experience with emerging technologies, including user experience, server side code optimization, network decryption, and front-end browser performance. Jason's prior roles include field CTO for AppDynamics (now Cisco), executive director at JPMorgan Chase owning application monitoring, vice president at BigPanda, and technical leadership positions at Mercury Interactive, Quest Software, and CA Technologies.

About Island

Island, the Enterprise Browser is the ideal enterprise workplace, where work flows freely while remaining fundamentally secure. With the core needs of the enterprise naturally embedded in the browser itself, Island gives organizations complete control, visibility, and governance over the last mile, while delivering the same smooth Chromium-based browser experience users expect. Led by experienced leaders of the enterprise security and browser technology space and backed by leading venture funds -- Insight Partners, Sequoia Capital, Cyberstarts and Stripes -- Island is redefining the future of work for some of the largest, most respected enterprises in the world. Island is based in Dallas with research and development in Tel Aviv and can be reached at info@island.io or (866) 832 7114.