EDITORIAL BRIEF

The Problems of Over-Permissive Privileges and How the Enterprise Browser Solves Them

By relocating the problem of controlling privileges to the browser, organizations keep their critical assets safer

By Murali Raju
Enterprise Architect

At a concert or sports event, fans can get passes that allow them to travel to areas that are off-limits to others in the venue: They can go backstage and visit the band or stand on the sidelines with coaches and players. In other words, they have access privileges.

This same concept applies within cybersecurity. Organizations must give their workers privileges to fulfill essential job functions. Sometimes these permissions or privileges go above and beyond what others in the organization have, because the worker in question has a specialized role. For example, they may be tasked with moving large sums of money and require exceptional privileges.

Yet just as someone with a general admission ticket isn't supposed to walk into a luxury box or visit backstage at a concert, organizations need assurance that workers are not going to unauthorized places or touching the wrong assets within their networks or systems.

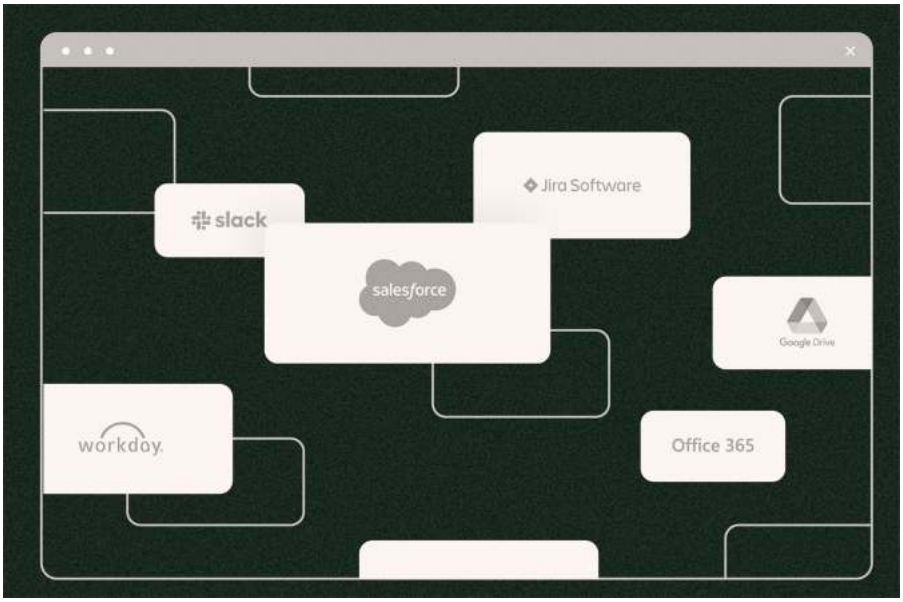
Unfortunately, the current methods for providing that assurance are fundamentally flawed – like a ticket taker who waves everyone through indiscriminately. User accounts within applications often have overly broad privileges because they cannot be customized for specific needs. This means that critical areas of applications are often governed no differently than the rest of the application.

The Limitations of Existing Methods for Governing Privileges

One of the core challenges organizations are facing regarding privileges is that they're limited by what their applications can do.

Applications typically have disparate capabilities. One application may let you govern who can login and who can't -- but once you're in, all bets are off and there is no control over who does what. Another application may have role-based access control, which prevents users from accessing things outside their defined sphere. Role-based controls often suffer from a lack of granularity. Building in extra control that is triggered when a worker attempts to process a financial transaction above a certain value, for example, can be difficult to accomplish.

This creates an environment of non-uniformity right out of the gate. Many applications – especially custom applications built years ago – were not designed with



An enterprise browser allows you to deliver very specific oversight of admin or privileged user accounts on existing applications.

Island

control in mind. Making changes to these internal apps (or to SaaS applications, which are built for the public and are not tailored for the specific circumstances of one business) is often difficult bordering on impossible.

Often the teams that built these internal apps five or even ten years ago are no longer around to make the changes you require. Adding new control features into a SaaS app can present complex challenges, and in many cases the vendor is too busy to provide timely help.

Another key limitation is visibility. While control and oversight are important, the ability to create a detailed record of user activity that can be referenced or investigated is also imperative. Often organizations have very little visibility into the operations of their privileged users. Many applications do not offer detailed audit logging, so it's impossible to create a record of who did what, who touched what, which changes occurred, who made the change, etc.

Because consumer browsers don't offer audit functionality, organizations are forced to rely on a disparate mix of applications to provide as much insight as possible. Without a unified process, attempting to manage logs and understand what has happened is expensive, time-consuming and largely ineffective.

While solutions such as Privileged Access Management (PAM) tools provide a level of control, they are both expensive and a separate area of tooling. They also typically feature considerable gaps, as they don't always cover all critical areas. Ultimately, PAM technology is meant to be a wrapper around applications that creates a bit more uniformity -- but it's expensive and an incomplete solution.

One of the core challenges organizations are facing regarding privileges is that they're limited by what their applications can do

How An Enterprise Browser Solves the Problem of Privilege Management

The Web browser is where users touch things that are critical parts of application flows, and as such, it's the perfect place to introduce governance. However, consumer-grade browsers have historically ignored these issues, instead focusing on speed and user experience.

Today that is changing, with the emergence of the first true enterprise browser capable of allowing organizations to exert granular control over privileges. It does this in part by validating logins, checking both user identity and the posture of a device and altering workflows of a given application to insert additional layers of security governance – without developer interactions.

The ability to add new workflows and dynamically change the behavior of an application is unique to an enterprise browser. In addition to asserting two-factor authentication, governing what users can and can't do in the application, and governing whether they should be able to login based on the device and their identity, an enterprise browser also provides visibility via auditing.

Instead of using standard logging for general purpose interactions via an application, an enterprise browser collects in-depth data about what users changed or touched. If a user goes to a critical area of an application and clicks a button or changes data, the browser can take a snapshot. This allows organizations to quickly generate answers to key questions such as

- Did a user copy data?
- Did they paste it somewhere else?
- Did they try to save a file?
- Did they download something, or did they save content?

This level of forensic auditing allows enterprises to quickly identify any security issues and then take immediate steps to address them.

The Takeaway

By introducing the ability to easily insert new workflows into any application, organizations can use enterprise browsers to do things that have never been done before.

An enterprise browser allows you to deliver very specific oversight of admin or privileged user accounts on existing applications, deeply monitor those key interactions, provide contextual logging, and insert MFA into a process flow where it otherwise did not exist.

This can eliminate the cost of convening an entire team (some of whom may be long gone) to change workflows and unlock granular control over application functions.

Ultimately, by relocating the problem of controlling privileges to the browser, organizations keep their critical assets safer – and make the process of maintaining effective governance vastly less expensive and time consuming.

About Murali Raju

Murali Raju currently serves as Enterprise Architect with over 25 years of experience in the industry. Prior roles include ranging from executive positions at Segment with a successful acquisition to Twilio, multiple series-D companies, to leading strategy, business incubation, M&A as part of the Office of the CTO at Cisco Systems, Inc.

Murali's early career began as a software engineer, developing embedded systems, then majority as an EIR (Entrepreneur in Residence) for private equity with responsibilities ranging from portfolio strategy, engineering, product, and GTM of businesses within multiple technology waves.

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