EDITORIAL BRIEF

Why Managing Contractor Access Through the Browser is Faster, Cheaper and More Secure

There is a better way to solve your contractor management issues: An Enterprise Browser.

By Jason Trunk
Enterprise Architect, Island Technology

Thanks to the exceptional flexibility they enable, contractors have become indispensable to the business models of many of today's leading companies. These benefits often come at the expense of cybersecurity, however. Many organizations have limited technological means to effectively govern contractors. The tools they use are overly complex, expensive, and ultimately not ideally suited to the task of effective contractor access oversight.

Fortunately, there is a better way to solve your contractor management issues: An Enterprise Browser.

Let's take a closer look at the problems with current contractor access management solutions, and how approaching these problems at the browser level helps organizations operate in a manner that is more streamlined, less costly – and ultimately safer for everyone.

Why Organizations Struggle to Manage Contractor Access

For security reasons, contractors should have their access limited to only those information resources necessary to perform their jobs.

Yet this is often easier said than done. Managing contractor access is often quite challenging given that they engage with your business, yet you don't typically control their devices. Getting contractors set-up on your organizational system, and governing their access effectively, can also be time-consuming, expensive and complex.

One common solution is to give contractors virtual private network (VPN) clients to access an environment. This forces their traffic back through your organization's controls and allows you to govern the things they touch.

Island

Yet there is a fly in the ointment: Many of the things that are most frequently touched are cloud applications and web-based services Thus by putting contractors onto your VPN, you slow down the process of getting them provisioned for the simple things they need to do their jobs. Further you are adding to the attack surface area that has access to your network resources.

Provisioning contractors with virtual desktop infrastructure (VDI) is another option. In this scenario, contractors are given their own virtual PC where they login to an operating system only to immediately launch a web browser, usually with increased latency and lower screen resolution. This approach is very pricey, not environmentally friendly, and is another layer of management for the IT staff --all to get to a website.

Overall, current solutions are best characterized as overly complex, expensive, too hard to deploy and insecure because they do not allow you to rapidly provision a new contractor, nor control and govern effectively.

Other Critical Contractor Access Challenges Organizations Face

Now that we've reviewed some of the limitations of conventional contractor management tools, let's review some of the key challenges organizations are facing in the absence of a better solution.

Working With Multiple Companies

Contractors often work with multiple companies, which could mean they are using more than one VPN or commingling data. They may have several tools from different companies with varying requirements on a single laptop. For the contractor, managing all of this becomes quite difficult. For the organization, security is a serious concern.

The Struggle to Separate Professional and Private Use

Another core concern with contractor access is overlap between private and professional use. When contractors use the same device for personal and professional activities, it often becomes very difficult to manage this situation in a way that respects privacy and protects the assets of the organization.

Content uploads from contractor devices cannot be easily inspected before insertion into an application. Corporate data being downloaded can land on unmanaged contractor devices, creating regulatory and privacy issues. Organizations must also weigh data sovereignty challenges to answer how data is safely stored and revoked, and auditing must be performed over contractor work activities within an application but not over personal interactions.

Governance Problems

Currently, policy management is driven by user identity with no consideration of device type. Ultimately, governance needs to be driven by more than just contractor identity – you can't effectively govern access without any consideration of the type of devices coming in on and separating their devices by policy from the ones used by your own employees.

Organizations can also apply role-based access controls, limiting access to various apps. Yet once a contractor is in the app, they're in the app. You must trust that they are not going to manipulate data or misuse data, innocently or otherwise. Without more granular or tactical control over policy enforcement, you are at risk.

Ultimately, organizations need a tool that gives them the flexibility to allow different categories of contractors to access the varying applications and services they need, while enabling the creation of guardrails that prevent them from crossing into areas where they don't belong.

Limited Flexibility

Contractors currently have limited workflow and security flexibility. Data redaction in key areas may require changes to application code or complex tokenization. Right now, there is no way to easily modify workflows of packaged SaaS or internal apps for contractor needs.

Lack of "Last Mile" Visibility and Control

Organizations have no way to prevent contractors from copying and pasting sensitive information or taking screenshots. This is one of the most glaring – and possibly damaging – limitations of existing contractor access management approaches.

How the Enterprise Browser Provides a Better Path Forward

What if, instead of using the traditional VPN/VDI approaches, organizations chose to manage contractor access within the actual browser?

The answer is simple: Those organizations would unlock a powerful new set of advantages that make contractor access management profoundly easier.

Unlike your typical consumer browser, an enterprise browser is built to work with your enterprise. It includes technology that allows an organization to gain critical visibility into how users behave within their browser and how they interact with applications.

An enterprise browser eliminates the unnecessary complexity and expense of VPN and VDI solutions and allows for the fastest deployment possible.

It can determine user and device posture upon launch, allowing the contractor to safely interact with the apps and data they need to touch to fill their role. This eliminates the problems of using an identity or role-based approach and delivers the tactical level of control needed for effective governance.

Additionally, an enterprise browser offers deep audit logging on the contractor's interactions with critical application areas, while still ensuring privacy for personal device use. This creates simplified and safer contractor provisioning while maintaining support for key applications.

Other key benefits include:

- Contractors can begin work in minutes, not days or weeks
- Device posture ensures identification of contractor specific devices where they are in use
- Granular policy enforcement driven by identity and device type provides superior governance to provide extensive guardrails unique to contractors
- Downloaded files cannot escape from critical apps onto user-owned devices
- Last mile controls prevent copy and pasting, saving page content, screenshots and printing
- Malicious files are scanned to prevent their upload to corporate apps
- Separating user personal and work interactions ensures privacy, as you can only audit corporate action logs
- Professional and personal personas can be easily maintained with data separation and anonymization ensuring simplified data sovereignty and regulatory compliance
- Reduced environmental footprint, moving away from reliance on cloud proxies, cloud zero trust networks, shipping laptops, and VDI server farms

An enterprise browser eliminates the unnecessary complexity and expense of VPN and VDI solutions and allows for the fastest deployment possible.

What if, instead of using the traditional VPN/VDI approaches, organizations chose to manage contractor access within the actual browser?

The Takeaway

Contractors have never been more vital to the operation of global business. Yet the limitations of conventional methods for managing their access to organizational environments mean that businesses struggle to securely give access in a very easy fashion.

Ultimately, approaching the problem of contractor access at the browser level allows organizations to reduce complexity, provision contractors almost instantly, save money, deploy far more quickly, protect privacy for all involved – and most importantly, keep critical assets secure.

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

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.