

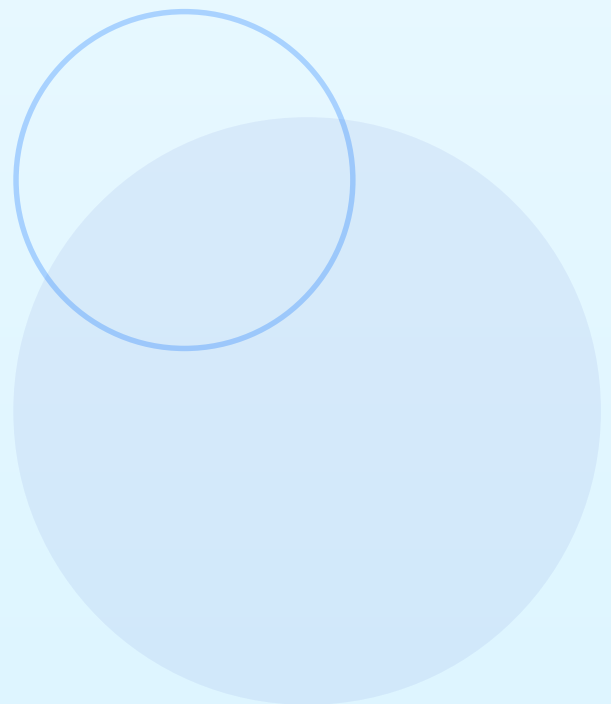
Enterprise Browser Analysis: Overcoming Security Gaps

Are they the right choice for BYOD workforces?



Table of Contents

• INTRODUCTION	3
• UNDERSTANDING THE TWO DIFFERENT PARADIGMS FOR BYOD WORKFORCES	5
• EXPLORING LIMITATIONS AND CHALLENGES OF ENTERPRISE BROWSERS	6
• COMPARATIVE ANALYSIS: CONCEPTUAL FRAMEWORK	9
• CONCLUSION	14



Introduction

In today's dynamic world, the conventional workplace paradigm is being reshaped by three macro trends: increasingly geographically dispersed workforces, the rise of the gig economy, and the ever-blurring line between work and personal life. This new landscape has fostered a surge in offshore workers, contractors, freelancers, and remote employees who use their personal devices for professional tasks.

The Bring Your Own Device (BYOD) workforce is now a reality, offering both challenges and opportunities for businesses.

As companies rely more on contractors and offshore workers, they naturally adopt BYOD policies to avoid the costs and logistics of shipping and tracking company-owned devices. The benefits are clear: streamlined onboarding and offboarding processes, reduced hardware expenses, increased agility, and the ability to hire talent from anywhere in the world. Embracing a BYOD workforce also gives employees more freedom.

However, this shift also presents new challenges. IT teams now face the pressing need to support and secure company data on a variety of unmanaged devices, recognizing that the traditional reliance on rigid, locked-down corporate computers is no longer sufficient.

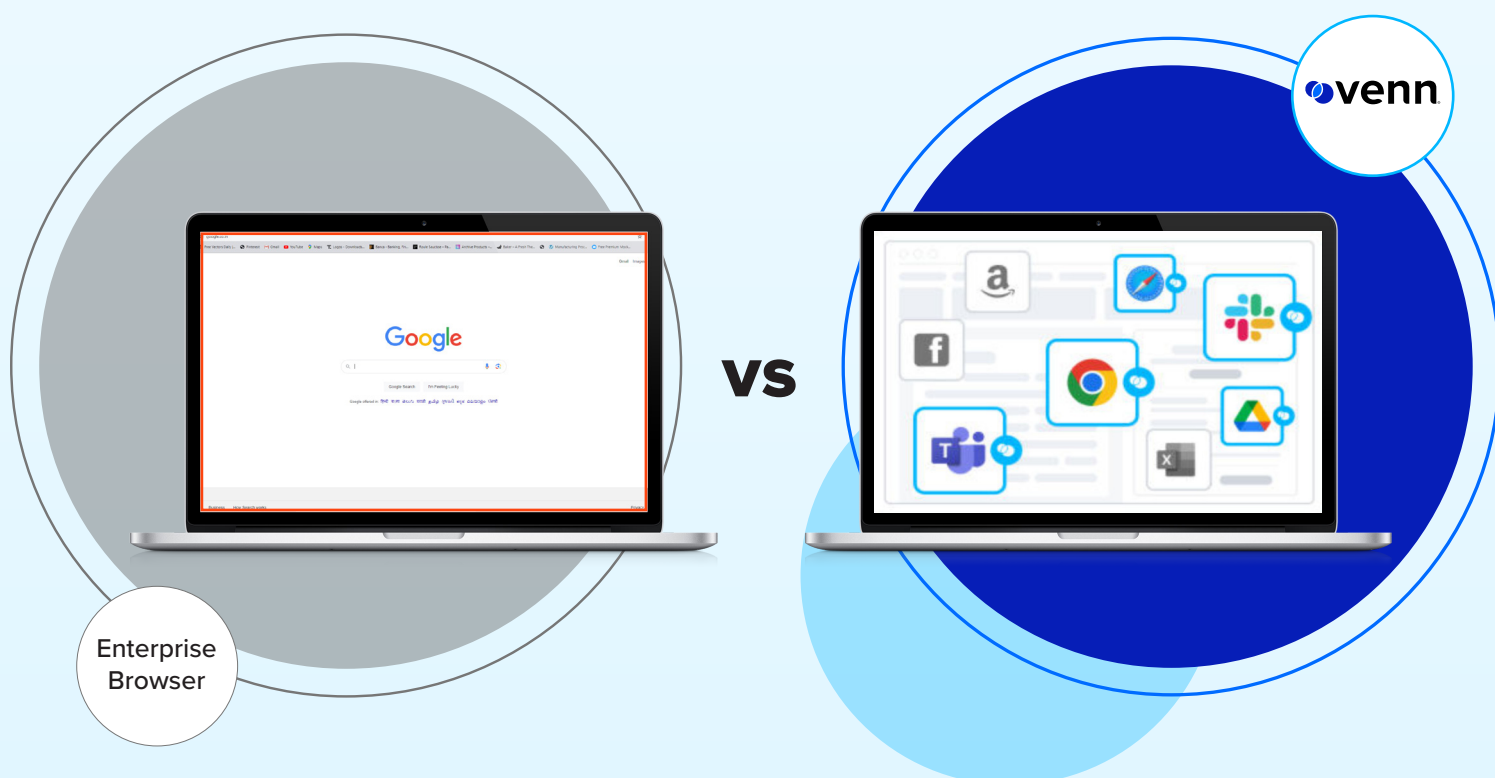


Introducing Two Paradigms: Enterprise Browsers vs. **Venn's Blue Border**

The emergence of BYOD workforces has underscored the need for robust solutions that enable productivity while maintaining stringent security protocols.

Enterprise browsers have become a popular choice for facilitating secure browsing and accessing web-based applications, especially in BYOD and contractor scenarios. These browsers provide a layer of security that helps protect sensitive information and ensures compliance with corporate policies.

Similarly, Venn's BYOD workforce enablement solution secures contractors and remote workers on personal or unmanaged devices, but in a completely reimagined way. In the following sections, we will explore both the strengths and limitations of these solutions to help IT leaders make informed decisions.



Understanding the Two Different Paradigms for BYOD Workforces

In order to understand the differences between these two computing solutions, we must first explore the fundamental distinctions in their approaches.

Enterprise browsers

Enterprise browsers are specifically engineered to cater to browsing activities and accessing web-based applications. They do this by creating a controlled browser environment where security policies can be enforced, such as blocking malicious websites, managing browser extensions, and ensuring secure connections.

Enterprise browsers provide a layer of security and convenience, particularly for tasks such as accessing cloud-based software and browsing the internet, and as such are beneficial in certain BYOD scenarios.

However, enterprise browsers typically do not address the security needs of locally installed applications or the protection of sensitive data stored on personal devices. This can leave organizations vulnerable to security breaches and compliance issues, especially in environments where users rely on a mix of web-based and local applications.

Venn's Secure BYOD Solution

Venn's secure BYOD solution offers a purpose-built approach to fortifying remote work on unmanaged or BYOD devices.

By establishing a Secure Enclave on the user's device, **Venn protects not only browsing activities, but also the local applications, files, and network.** This holistic approach ensures that all business activities, whether conducted on a browser or otherwise, are secured.

Venn utilizes secure containers to completely isolate business and personal information, ensuring the protection of sensitive company data and personal privacy. This mitigates security risks and enhances efficiency without sacrificing the end-user's native experience.

By understanding the fundamental distinctions between enterprise browsers and Venn, IT leaders can better evaluate which solution aligns with their organization's needs in enabling secure BYOD workforces.

Exploring Limitations and Challenges of Enterprise Browsers

The core message gleaned from discussions with industry experts and prospects is clear: Enterprise browsers are proficient at handling web-based applications and provide a valuable layer of security for online activities. However, they may encounter challenges in meeting the diverse demands of complex work environments.

Here are limitations and challenges sometimes faced by organizations utilizing enterprise browsers.

1

User adaptation challenges with web-only restriction



Enterprise browsers are specifically designed to support web-based applications, which significantly limits their utility in real-world work environments where employees rely on a variety of software tools.

Many people prefer using local applications like Outlook, Office, Zoom, Slack, and downloading files locally, rather than relying solely on web-based solutions such as OneDrive. This preference is reflected in the continued popularity of Windows and Mac machines for personal use as opposed to Chromebooks. Transitioning entirely to browser-based operations can create friction as it requires significant changes in user habits.

Essential applications such as Microsoft Office, Slack, and Zoom, which are critical for everyday operations, typically run locally on devices and are not supported within the confines of an enterprise browser. This restriction forces employees to juggle between secured and unsecured environments, complicating their workflow and, more importantly, risking the security of company data.

As a result, the enterprise browser's web-only focus fails to accommodate the comprehensive application needs of a diverse and dynamic workforce.



2

Security gaps



While enterprise browsers provide a certain level of security for activities conducted within the browser itself, they fall short in protecting local applications and data stored on employees' devices. This creates significant security gaps, as sensitive information can be exposed when employees switch between the secure browser and unprotected local applications.

Many companies assume that SaaS solutions fulfill all their employees' work needs and therefore believe enterprise browsers to be sufficient. However, upon closer inspection, they often discover that employees also rely heavily on locally installed applications, revealing a significant oversight in their security strategy.

The inability to provide consistent security coverage across all work-related activities makes enterprise browsers an incomplete solution for safeguarding company data, leaving organizations vulnerable to data breaches and other cyber threats.

3

Compliance challenges



Ensuring compliance with industry regulations and internal policies is a critical concern for businesses, especially when employees use their own devices for work.

Enterprise browsers offer limited compliance measures that only apply to web-based activities, neglecting local applications and data. This incomplete compliance coverage poses significant risks, as organizations may struggle to enforce and monitor compliance standards across both browser and local environments.

The complexity of maintaining comprehensive compliance can lead to regulatory breaches and legal repercussions, undermining the organization's integrity and operational stability.

4

Inability to support legacy systems



Enterprise environments are characterized by their complexity, often featuring a multitude of installed applications. Many of these applications are legacy systems that cannot be easily replaced with modern, web-based alternatives. But these applications tend to be deeply integrated into critical workflows and processes, making them indispensable despite their outdated technology.

Attempting to force a browser-only solution in such environments would not only disrupt established workflows but also risk compromising the productivity and security of the organization. In such cases, relying on an enterprise browser would hinder companies from supporting contractors and employees who need access to these particular tools.

Against this backdrop of challenges and limitations with enterprise browsers, Venn's secure BYOD solution offers a paradigm shift that enables a secure & local end-user experience. By creating a secure enclave on the user's device, Venn ensures the encapsulation of all business-related activities, shielding them from potential security breaches or compliance lapses while providing a seamless user experience.













Comparative Analysis: Conceptual Framework

Regulation	Criteria	Venn	Enterprise Browser
Security and Compliance	Can users perform their usual workflows without either accidentally or maliciously exposing sensitive company data?	★★★★★ DLP controls and Secure Enclave ensure no accidental or malicious data exposure, while enabling usual native workflows.	★★★★ Limited protection outside the browser leaves potential for accidental or malicious data exposure.
	Can users utilize web and local apps, as well as save files locally in a secure way?	★★★★★ Venn supports the protection and isolation of both web and local apps, with secure local file saving within the Secure Enclave.	★★★★ Enterprise Browsers only support web apps, lacking the ability to secure workflows of local apps or save files locally.
	Is data protected at rest, in motion and in use?	★★★★★ Venn ensures data protection at rest with an encrypted file system, isolates and encrypts data in motion, and restricts access to authorized work applications.	★★★★ Data protection is limited to isolation while in use, with potential exposure through freely uploading/downloading files and accessing data over any network unless browser policies are implemented.
	Can a user unknowingly expose company data?	★★★★★ Venn's DLP controls mitigate most user actions that could expose company data, though data could still be sent outside the enclave via email without additional content filtering controls.	★★★★ Similar to Venn, DLP controls limit exposure from most user actions, but data could still be exposed via email without additional content filtering controls.
	Can malware and viruses access company data?	★★★★★ Venn isolates work applications and data from personal ones, verifies applications before use, and integrates with virus tools to protect files moved within the enclave.	★★★★ Web applications and data are isolated from the local system, employing safe browsing techniques and integrating with virus tools to protect downloaded files.

Regulation	Criteria	Venn	Enterprise Browser
	Is security and compliance reportable and demonstrable?	 <p>Venn allows configuring device, application, web, and DLP policies to align with company policies, with dashboards, audit trails, and prebuilt compliance reports providing real-time visibility.</p>	 <p>Solutions in this category offer centralized auditing and reporting for web applications only, lacking visibility into company data accessed by local applications.</p>
User Convenience and Privacy	Can users utilize a single computer for both work and life without negatively impacting their user experience or performance?	 <p>Venn ensures seamless integration of work and personal use on a single device, maintaining user experience and performance.</p>	 <p>Limited support for work and personal use on the same device, since Enterprise Browsers only support web-based activities.</p>
	Can users follow their usual flows without having to significantly change the way they use their computers?	 <p>Yes, users will use the same applications, in the same way they do now. No retaining or switching workflows required.</p>	 <p>No, users of local applications need to find an online version of the app or use a different web app. In both cases, users will need to adapt to the online version or learn a new app.</p>
	Can a user choose their own device?	 <p>Venn supports Windows, macOS, iOS, Android.</p>	 <p>Support across multiple platforms is available, but browser choice may be limited to Chromium-based options in most cases.</p>
	Can a user expect the same experience and performance of their applications without experiencing lags or delays?	 <p>Venn ensures consistent performance of applications within its local Secure Enclave, minimizing lags or delays.</p>	 <p>Performance may vary, potentially leading to lags or delays depending on the device used.</p>
	Can a user safely use the computer for work and personal use?	 <p>Venn's Secure Enclave ensures safe usage for both work and personal activities on the same device.</p>	 <p>Limited security measures outside of the browser may pose risks for using the same device for work and personal use.</p>

Regulation	Criteria	Venn	Enterprise Browser
	Is personal privacy assured and demonstrable?	 <p>Venn prioritizes personal privacy and provides complete separation of work and personal. Your company will never be able to access or monitor your device's usage outside of the Blue Border.</p>	 <p>Privacy levels are communicated to the end-user, but complete privacy is not assured.</p>
	Can users seamlessly utilize common every-day SaaS applications like Zoom and Slack?	 <p>Venn ensures seamless integration and usage of popular SaaS applications like Zoom and Slack within its Secure Enclave.</p>	 <p>Usage of common SaaS applications may be hindered by limitations within enterprise browsers, potentially impacting user experience and performance.</p>
Cost	Does the solution cut down on hardware and management costs for remote employee computing devices?	 <p>Venn's solution significantly reduces hardware and management costs associated with remote employee computing by eliminating the need for extensive hardware investments and simplifying management.</p>	 <p>Enterprise browsers also contribute to cost reduction by streamlining device management.</p>
	Is there flexibility to move to new employee computing approaches such as bring your own computer (BYO)?	 <p>Venn offers full support for new employee computing approaches like BYO, providing flexibility for organizations to adapt to evolving workforce preferences.</p>	 <p>Enterprise browsers similarly support BYO approaches, ensuring flexibility in employee computing choices.</p>
	Are backend infrastructure costs reduced, or eliminated, to support and manage physical or virtual devices?	 <p>Venn's solution helps reduce backend infrastructure costs by simplifying device management, though some infrastructure may still be necessary for optimal performance.</p>	 <p>Enterprise browsers contribute to significant backend infrastructure cost reduction, particularly in virtual device management scenarios.</p>

Regulation	Criteria	Venn	Enterprise Browser
	Do other products need to be purchased for a complete solution?	 <p>Venn provides a comprehensive solution without the need for additional purchases, ensuring a complete and integrated approach to BYOD workforce security.</p>	 <p>While enterprise browsers offer core functionality, additional products or services may be required to achieve a complete solution, potentially leading to additional costs.</p>
Control	Does the solution allow centralized security and IT policies, and remote management of devices?	 <p>Venn enables centralized security and IT policies, along with remote management of devices, providing comprehensive control over BYOD work environments.</p>	 <p>While enterprise browsers offer some degree of centralized security and IT policy management, remote device management capabilities may be more limited.</p>
	Is there a central point of control for device, user and application policies?	 <p>Central point of control for device, user, and application policies, ensuring consistent and unified management across the BYOD workforce.</p>	 <p>Centralized control for device, user, and application policies, allowing organizations to enforce security measures consistently.</p>
	Is there support for installing and managing local applications on the device remotely?	 <p>Venn supports remote installation and management of local applications on devices, streamlining administration and ensuring software compliance.</p>	 <p>Enterprise browsers do not secure local applications in any way; they only secure what happens inside the browser.</p>
	Is there control over local and SaaS applications?	 <p>Venn provides control over both local and SaaS applications, allowing organizations to enforce security policies uniformly across all application types.</p>	 <p>While enterprise browsers offer control over SaaS applications, control over local applications is minimal at best, creating security gaps.</p>
	Is there control over DLP?	 <p>Venn offers robust control over Data Loss Prevention (DLP) measures, ensuring sensitive data is protected across the BYOD workforce.</p>	 <p>Control over DLP measures within enterprise browser environments may be effective but could vary in comprehensiveness compared to Venn.</p>

Regulation	Criteria	Venn	Enterprise Browser
	Is network traffic controlled?	 Venn enables granular control over network traffic, ensuring secure communication channels and mitigating potential security risks.	 While enterprise browsers offer some degree of centralized security and IT policy management, remote device management capabilities may be more limited.
Easy Deployment	Is there self-service deployment and easy integration with 3rd party IT and security SW?	 Venn offers self-service deployment and seamless integration with third-party IT and security software, simplifying the setup process and enhancing overall efficiency.	 Enterprise browsers provide self-service deployment options and integrate with third-party software, though the integration process is less streamlined.
	Are users able to self-onboard?	 Venn allows users to self-onboard easily, reducing the administrative burden and accelerating the deployment process.	 Users can self-onboard with enterprise browsers, though the process may not be as intuitive.
	Is integration with other products needed for a complete solution?	 Venn provides a comprehensive solution that minimizes the need for additional product integrations, ensuring a streamlined deployment.	 Enterprise browsers often require integration with other products to form a complete solution, potentially complicating deployment and increasing costs.
	Is integration available with best of breed products, such as 3rd party IDPs, SASE, VPNs, MFAs, MDMs, and file systems?	 Venn supports integration with a variety of best-of-breed products, including third-party IDPs, SASE, VPNs, MFAs, MDMs, and file systems, providing a flexible and interoperable solution.	 Integration with products is possible with enterprise browsers, but is not as seamless as Venn.

Conclusion

Recap

In reviewing the comparison between Venn and Enterprise Browsers, it becomes evident that both solutions offer distinct approaches to addressing the security challenges of BYOD work environments.

Venn's secure BYOD solution stands out for its comprehensive security measures, encompassing both web-based and local applications, which empowers organizations with a holistic approach to data protection and compliance.

On the other hand, Enterprise Browsers, while suitable for basic browsing tasks, may fall short in addressing the diverse application needs and security requirements of modern work environments.

Recognizing the strengths and limitations of each solution enables organizations to make informed decisions that best suit their specific needs and priorities in supporting BYOD workforces.

Future outlook for BYOD workforce solutions

Looking ahead, the landscape of BYOD workforce solutions is poised for continuous evolution and innovation. As more contractors and employees start utilizing personal computers for work, there will be a growing demand for adaptable and user-friendly solutions.

Venn's approach to securing remote work on BYOD devices sets a precedent for future developments in this space. By prioritizing security, compliance, and user experience, Venn offers a blueprint for organizations navigating the complexities of BYOD workforces in a post-pandemic era.

However, Enterprise Browsers are likely to continue evolving to address the changing needs of BYOD work environments, potentially offering enhanced features and integrations to meet the demands of diverse workforces.

Ultimately, the key to success lies in embracing flexible and scalable solutions that empower employees to work efficiently from anywhere, while safeguarding the integrity of corporate data and operations.





Thank You

Want to learn more about how Venn can secure your BYOD workforce?

[Book a short demo](#)

And be sure to follow us on socials for the most up-to-date news.

