Island

VDI Solution Brief

Is it Time to Rethink VDI?

Two decades ago, the promise of a centrally managed and widely distributed virtualized desktop was irresistible. This innovative technology promised a consistent way to deliver applications to end-users with convenient access controls and good security protections. At the time, the relative performance advantage of enterprise-grade servers over desktop PCs made the user experience of VDI a reasonable substitute for locally-installed applications. It's no surprise that VDI leaders like VMware and Citrix gained significant adoption.

Today, the enterprise landscape is completely different. Most applications are hosted in the cloud and delivered through a browser. Desktop PCs are dramatically more capable and much faster. Phones and tablets make mobile computing more convenient with fewer limitations. The era of spatial computing and enterprise VR/AR seems just around the corner. Against this backdrop, it's time for CIOs to adjust their virtualization strategy. In short, it's time to rethink VDI.

Advantages of VDI

VDI clearly holds several advantages over traditional desktop management that drove its adoption. The question for today is whether those advantages are aligned with the high cost of VDI — and whether those same advantages can be found with alternative technologies.

Centralized Management

Virtualized desktops offer the advantage of centralized management of widely distributed users. VDI also makes it possible to onboard new users without provisioning new hardware. This separation between the endpoint device and the virtualized operating system creates an efficient model for centralized management.

Secure Access

Virtualization presents a reduced attack surface by storing the OS, applications, and data on a centralized server rather than each endpoint. When paired with regular maintenance, this reduces risk from unpatched software. VDI access is typically integrated with enterprise identity management systems to reduce risk from unauthorized access.

Consistent User Experience

A virtualized desktop offers a consistent user experience regardless of which device they're using, including BYOD in some cases. Depending on the VDI implementation, virtual desktops can be persistent and customizable by the users (just like a regular desktop) or they can be non-persistent, meaning that the system resets to its original state with every session login.

Costs of VDI

The centralized nature of VDI architecture makes it a relatively high-cost solution. Because it's a central part of the user workspace, the costs extend beyond direct hardware and software into indirect end-user costs. Against the comparison of legacy technologies and applications from decades past, these costs may represent a worthwhile investment. In the context of a modernized enterprise workspace with compelling alternatives, these costs are hard to justify.

Infrastructure

Virtualizing a large number of desktop applications requires significant server infrastructure. Whether hosted in a private data center or through a cloud provider, the compute requirements of virtualization will always carry a high price point. While there are some scaling efficiencies, this infrastructure expense grows along with user count.

Administration

Managing, maintaining, and optimizing desktop virtualization platforms requires highly specialized skills across a range of domains. According to recent research published by Forrester1, "A common complaint in the VDI space is the tacit requirement for dedicated staffing, even from VDI admins themselves. As end-user computing and remote work teams are already stretched thin, something "simpler to manage" is at the top of every team's wish list." For on-premise VDI, this includes infrastructure maintenance and management. Cloud VDI or DaaS shifts the burden to configuration and optimization specialties. Cloud DaaS is typically sold with consumption-based pricing, so the degree of optimization will directly impact the overall cost of the system. As an example from the same Forrester research1, "One customer reported getting nonpersistent instances down to $4 per user per month compared with its previous average of $40 per user per month." This 10-fold price difference makes clear the importance of optimization of any virtualization platform for the specific workflows and usage patterns in the organization.

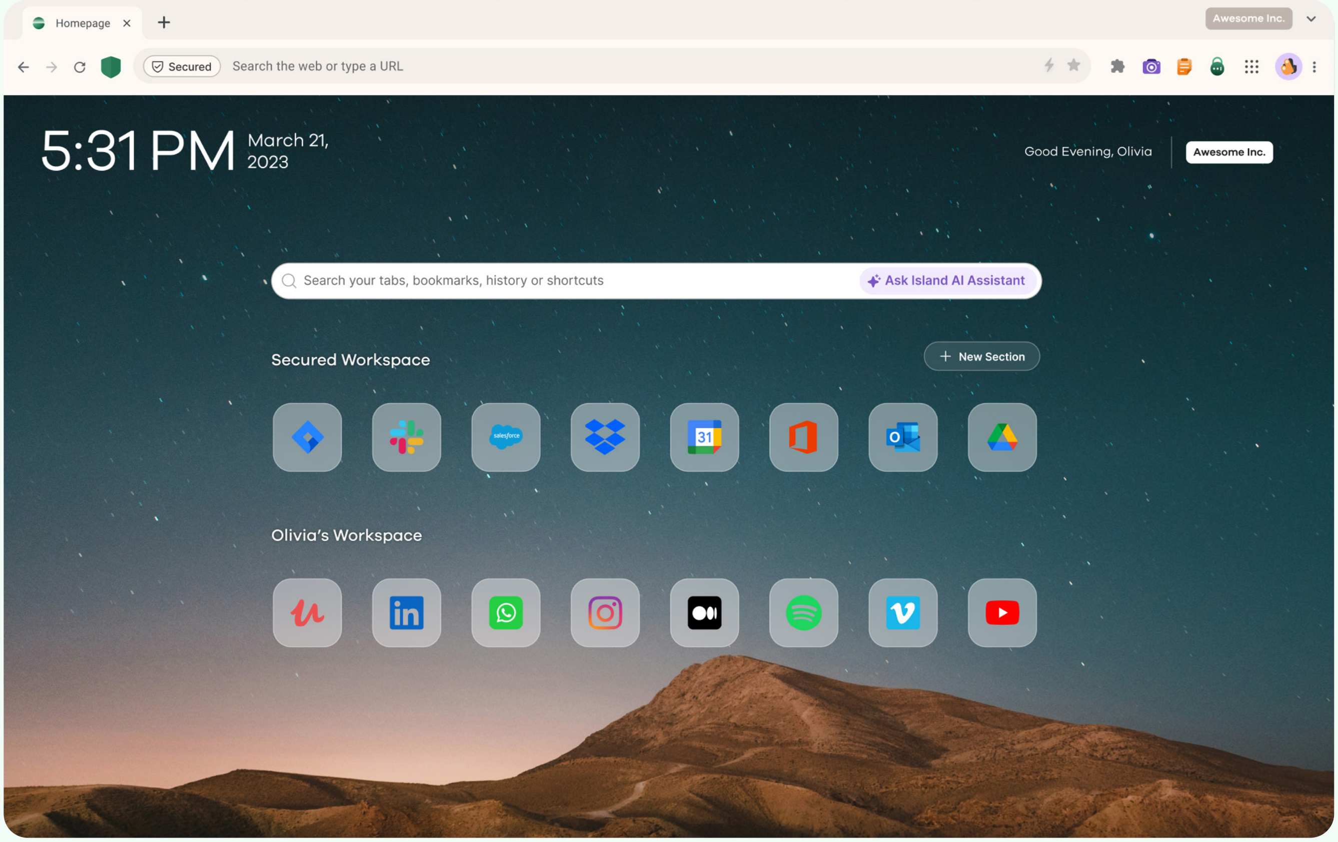
End User Productivity

Arguably the most significant cost to consider is the most difficult to measure: end user productivity. The increased friction added by the virtualization layer is a tax that every employee must pay, every day. Login delays, session interruptions, performance issues, and compatibility challenges combine to slow down daily work and cause user frustration. Add to this cost the Help Desk staff who are responsible for troubleshooting and resolving these hindrances and the total cost is significant.

Enter, The Enterprise Browser

The Enterprise Browser is not a desktop virtualization platform; it's an enterprise workspace designed for modern workflows, where most applications are accessed through a browser. With unique data protections, access controls, and a robust security policy framework, it can deliver many of the same advantages as VDI without the large infrastructure requirements — and associated costs. For legacy applications that require virtualization, the Enterprise Browser can also serve as the endpoint client for virtualized applications. Most importantly, the Enterprise Browser offers a dramatic improvement in user productivity, replacing a friction-heavy VDI experience with a natural workspace that's optimized for enterprise work.

> *49% of global employees in Forrester's Workforce Survey, 2023, say that they can do all of their work in a web browser;*



Delivering the Same Advantages as VDI

Centralized Management

åThe Enterprise Browser is managed through a cloud-based management console where administrators can define policies, configurations, and access rules. Each browser within the organization communicates with the management console to retrieve policies and configurations which are then applied locally within the browser. This model improves upon VDI by allowing direct application access (e.g., to SaaS applications) rather than rerouting all traffic through a centralized virtualization platform.

Secure Access

Like VDI, the Enterprise Browser integrates with enterprise identity management systems to authenticate users and provision access. The Enterprise Browser enables zero trust access, considering many factors like user identity, device configurations, network connection, and geographic location. Similar to VDI, the Enterprise Browser offers a layer of separation between the endpoint and the applications within the browser. Applying last-mile controls means that sensitive data is kept within enterprise applications, not downloaded or saved to the endpoint.

Consistent User Experience

The Enterprise Browser is based on Chromium, the same browser technology that powers Chrome and Edge. This provides a familiar user experience that requires no additional training or special onboarding. Installing the Enterprise Browser can be done by end-users themselves (convenient for BYOD programs) or deployed with IT endpoint management tools. Unlike VDI, there's no virtualization layer to introduce latency and the browser can take full advantage of the available network and endpoint resources. Application performance is fast and frictionless.

Eliminating the Costs of VDI

Infrastructure

The Enterprise Browser installs locally on the endpoint — just like a traditional browser — and does not require significant backend infrastructure. The cloud-based management console allows for global configuration and policy management, but importantly it does not require proxying the network traffic. The unique architecture of the Enterprise Browser allows for full control and visibility of web activity without modifying the network traffic flow. This also means that application access with policy enforcement is truly universal, regardless of which device or which network is used.

Administration

The significant reduction in backend infrastructure likewise reduces the administrative burden for deploying and operating the Enterprise Browser. There are no servers to operate and maintain, no virtual desktop images to build and patch, and licensing costs are predictable based on user count rather than usage patterns. The Enterprise Browser requires administration, but the skills required are readily transferable for IT and security professionals with experience managing other enterprise services.

End User Productivity

Moving from VDI to the Enterprise Browser offers a dramatic improvement for end user productivity. First, by eliminating all the friction and performance issues common to virtualization. Beyond that, the Enterprise Browser offers key capabilities to enhance productivity: robotic process automation (RPA) can automate and optimize common workflows; an integrated AI Assistant speeds up research and writing; the Smart Clipboard retrieves commonly used phrases with a click. Unlike VDI, the Enterprise Browser offers deep integration with SaaS and web applications to optimize business processes and deliver unmatched user productivity.

A Closer Look at The Enterprise Browser

Common web browsers are designed for the widest possible user community, with the majority of usage representing personal use by consumers. The Enterprise Browser differentiates from common web browsers by embedding IT, security, and productivity capabilities designed for the workplace. The user-facing Enterprise Browser is coupled with backend services and administration capabilities that provide the enterprise IT and security teams with additional configurability to tailor the Enterprise Browser for their specific business requirements and use cases.

Key Capabilities

- Access management with IdP integration that supports granular controls to protect specific applications, workflows, and data.
- Data protection policies to govern how data can move between or outside of applications.
- Conditional access policies to ensure that a device meets the organization's requirements before accessing critical SaaS applications.
- Data segregation and application isolation between an enterprise browser and the device it's running on to provide deployment flexibility with robust security.
- Integrated zero trust network access for secure connectivity to private applications
.
- Easy deployment of the Enterprise Browser to existing laptops or mobile devices using endpoint management tools or self-service by users.
- Full visibility of application access, security events, and data movements with integration to SIEM or other data analytics platforms.

Industry Experts View

Frost & Sullivan Radar

Published December 2023

Legacy VDI, VPN, and DaaS tools do not adequately support new forms of remote and hybrid work connectivity and end up delivering inefficient workflows and unintuitive user interfaces. Such challenges promote the adoption of modern and user-friendly ZTBS [Zero Trust Browser Security] solutions.

Gartner, Emerging Tech: Security — The Future of Enterprise Browsers

Published 14 April 2023

By 2026, 25% of enterprises will be using managed browsers or extensions, up from less than 10% today.

By 2030, enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience.

By 2030, the browser will become a platform from which enterprises can distribute software, collect intelligence, control access and securely enable remote work. In Phase 3, browsers will have evolved from a single application to a series of bundled applications and ultimately a platform from which other applications are run. Enterprises will routinely use secure, managed browsers as their primary control point for access. Applications will be seamlessly and securely delivered on demand within the browser tab structure, providing a consistent user experience with access to tools on nonweb ports and protocols.

Common Use Cases for VDI Reduction

Secure SaaS & Web Access

The shift to SaaS and web applications for a wide range of business means critical data and workflows move through the browser. A common browser offers very little in terms of security and data controls, forcing organizations to implement various measures outside the browser to try to stop data leakage and protect their applications. With an enterprise browser, organizations have a closed-loop system where security and access policies can be implemented across any SaaS and web apps. This ensures that data remains fundamentally secure, without relying on complex network controls, app-specific APIs or other solutions outside the browser.

BPO and Contractor Third-Party Access

As organizations supplement their employee workforce with contractors or business process outsourcers (BPOs), the challenge for efficient and secure access compounds. Two common approaches to solve this is provisioning managed laptops or setting up virtual desktops. The hardware route adds cost and delays, particularly when contracted staff are in foreign countries. Choosing a virtual desktop adds cost and complexity, with the added burden of a sub-par user experience and higher administrative overhead. An enterprise browser offers a superior choice, allowing contractors to use their existing hardware while maintaining full control over access, data security, and visibility. And unlike VDI, there's no performance penalty for the users.

BYOD Programs

Implementing a BYOD program that simultaneously satisfies business requirements, IT and security needs, and is practical and accepted by employees is a challenge that's vexed organizations for better than a decade. MDM solutions can satisfy the business and IT, but often meet resistance when employees discover the level of control they must give up on their personal devices. VDI solutions offer better segmentation between work and personal use, but come at a steep cost and impair the user experience. An enterprise browser balances the needs of all three constituencies with an elegant solution that is lower cost, easy to administer, and delivers a natural user experience while preserving personal control over the personal device.

Customer Example: Telehealth

A fast-growing telehealth company faced the challenge of onboarding thousands of contractor clinicians as they scaled to meet demand. Securing extremely sensitive patient data is mission critical. Purchasing, configuring, and shipping laptops was too slow and labor-intensive for their model. Desktop virtualization could work, but the cost of implementation and ongoing management was discouraging.

Instead, they chose Island, the Enterprise Browser. During onboarding, the clinician installs the enterprise browser on their computer and logs in with their credentials. They can immediately access all the apps they need to see patients and provide care. Patient data is safe and secure, always encrypted, and all browser data is wiped after every session.

Customer Example: Retail Point-of-Sale

A large U.S. retailer wanted to empower all their sales staff with mobile devices for point-of-sale transactions anywhere in the store. Data security is crucial for handling customer data and payment information. Their first attempt was to use Microsoft Azure Virtual Desktop to make a secure connection to the POS system. Usability problems hindered their rollout: AVD didn't work well with the on-screen virtual keyboard and the virtualization lag was noticeable. Virtualization could meet some of the security requirements, but at a steep cost to sales staff productivity.

Instead, they selected Island, the Enterprise Browser. The browser is installed natively on their Microsoft Surface tablets and connects securely to their POS system. Sales staff enjoy a much faster login process at the start of their shift and all the virtualization lag is gone. Customers are happy with a faster transaction and sales staff can get more done in a shift. Plus, corporate has more control and visibility than ever before, including a real-time screenshot of the receipt when a sale is booked.

Conclusion

Desktop Virtualization is a mature technology that unlocks powerful workflows, but comes with a steep cost and high complexity. Like any technology, it has strengths and weaknesses that must be balanced. On-prem VDI offers a high degree of control, but requires a massive infrastructure investment and specialized tools and staffing to maintain. DaaS moves some of the infrastructure to the cloud, but adds new complexities like performance and cost modeling. Either implementation gives end-users an experience that leaves much to be desired.

Over the past few years, a combination of forces made remote work and web-delivered SaaS applications commonplace. It's at this moment that organizations are rethinking their use of desktop virtualization in the name of efficiency and user experience. If your primary objective for virtualization is securing access to SaaS and in-house apps, The Enterprise Browser offers a new, modern alternative.