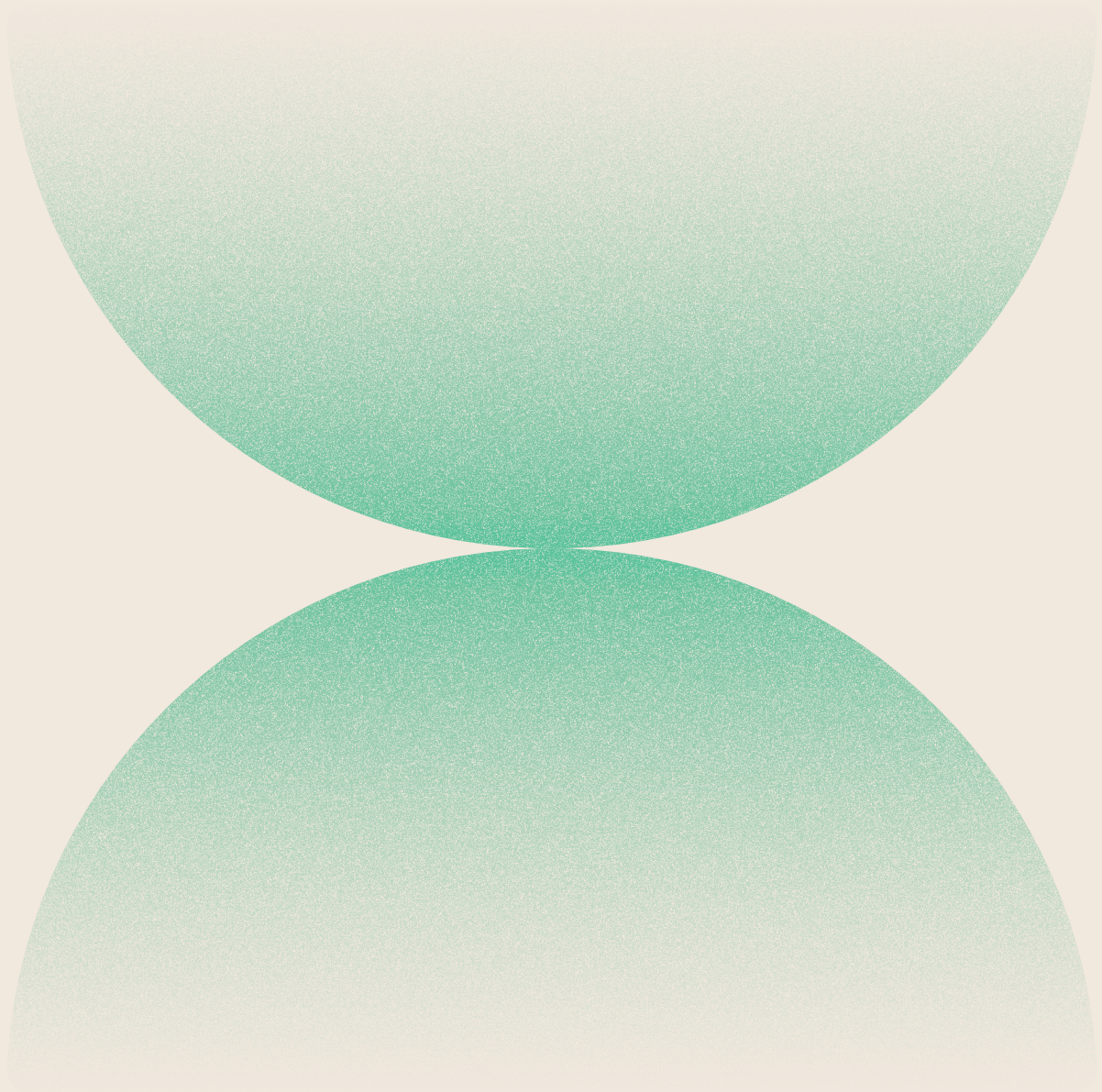




A Modern Alternative to VDI or DaaS for Secure App Access

Solution Brief | June 2022



Introduction

Desktop Virtualization was a remarkable innovation when it first came to market and quickly gained widespread enterprise use. Businesses enjoyed the flexibility in connecting employees with applications, data, and processing capabilities. Securing data was simpler with centralized servers rather than thousands of individual endpoints. Ubiquitous broadband networks made desktop virtualization possible from outside the office. VDI was the norm in the era of on-prem data centers and in-house apps. More recently, desktop virtualization moved to the cloud with Desktop-as-a-Service (DaaS) offerings. When the 2020 pandemic emptied offices around the world and forced remote working arrangements, many organizations dramatically expanded their use of desktop virtualization. Gartner reports that Desktop as a Service (DaaS) grew by 98% in 2020 compared to 2019.¹ Today, remote or hybrid work is the norm for many industries. Security and Operations leaders are re-evaluating their tech stacks to balance security concerns, operational costs, and end-user experience. In the case where information security and access controls are the primary driver for desktop virtualization, there's a compelling modern alternative: This paper explores where The Enterprise Browser can replace or augment traditional VDI or DaaS, and highlights the significant operational and cost benefits an alternative approach can bring.



¹ Market Guide for Desktop as a Service, Published 29 June 2021 by Gartner

Motivations for Desktop Virtualization

For the purpose of this paper, we define two broad categories of desktop virtualization. First, let's consider virtualization motivated by hardware limitations or capacity. Thin clients are a great example, where onboard storage and processing power is severely limited. Or, workflows that require high-end GPUs or exotic compute engines that are impractical or impossible to deploy to each employee who needs access. In these cases where the local hardware is insufficient for the workload, VDI is a good option. The larger category for virtualization is security motivated: workers connect to a virtualized desktop to access the apps, data, and services they need to get work done. In this case, the benefits of virtualization are primarily related to security and operations. With a centralized VDI or DaaS platform, the initial perception is that it's easier for operations staff to apply configurations, add or remove apps, and apply updates. Network configurations are simplified as well, with all traffic routing through the host servers. The pressure to support remote workers makes this even more important: desktop virtualization offers a practical approach to extend access to home-based workers, even those connecting from their personal (unmanaged) computers. Instead of opening a VPN tunnel and allowing every (unmanaged) endpoint on the network, a virtual desktop provides the management and security controls needed to protect apps and data.

desktop virtualization offers a practical approach to extend access to home-based workers, even those connecting from their personal (unmanaged) computers

The Downside

Up to this point, desktop virtualization sounds like a great solution. And for a time, it was! There are a number of solutions on the market from tech leaders like VMware, AWS, Microsoft, and Citrix. Plus a dozen or more smaller vendors that offer products to fit a particular niche. So why consider an alternative?

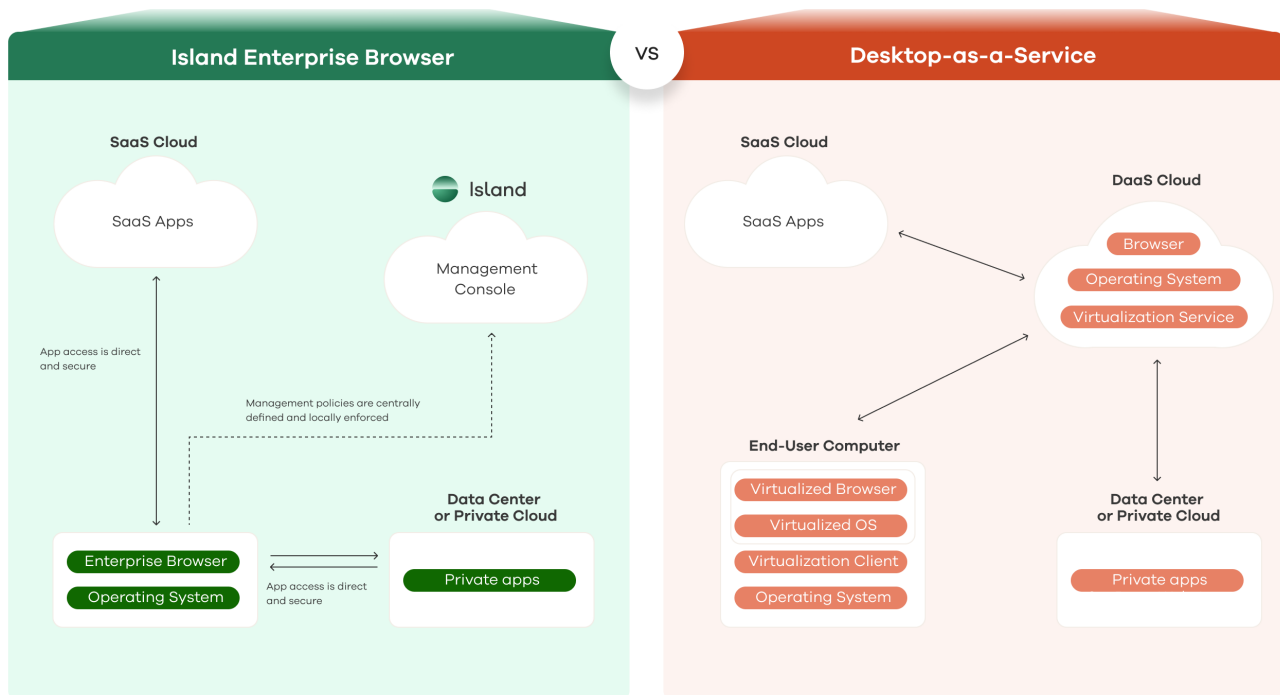
Cost

All the technology that makes desktop virtualization so compelling comes with a steep price tag. According to Gartner, a mid-tier DaaS costs \$50 to \$200 per user, per month². And that's on top of the cost of the computer needed to run the virtualization client. There are significant operational costs as well, with specialized tooling and skills required to manage the virtualized environment and optimize performance. Most DaaS offerings include variable costs, depending on actual usage, so performance and cost modeling are critical. If the virtualization strategy can offset substantial hardware costs, like high-end GPUs, then it probably makes sense. But when desktop virtualization is used for secure access to apps, and especially when those apps are delivered through a web browser, these costs can quickly outweigh the benefits.

² Price Range for Medium-Specification Shared Desktop OS (Medium Specification Shared Desktop OS 2 vCPU, 8GB RAM) as published in Market Guide for Desktop as a Service, Published 29 June 2021 by Gartner

User Experience

The same factors that we list as benefits for security and operations staff show up as costs to the end-user: offloading the application and data layer to a centralized service means every action by the user takes an additional round trip that adds some lag. In the real world of noisy wifi networks and bandwidth-constrained connections, the user-experience can be dreadful. Worse, a dropped connection often requires re-authentication that can add painful delays in getting work done.



This product review published on G2.com gives a sense of the end-user frustration:

“ This software requires an internet connection and provides a virtual desktop. We have a Fiber connection at my home and reliable and fast internet, even so, I find that there is a significant lag when using the Citrix desktop. It is difficult to switch between applications. Even the most simple tasks such as creating a document are hindered by the lag. There is a distinct lag in even getting your cursor at a specific place in the document. Tasks that are usually simple, such as resizing a screen in Windows are slow and bulky. ”

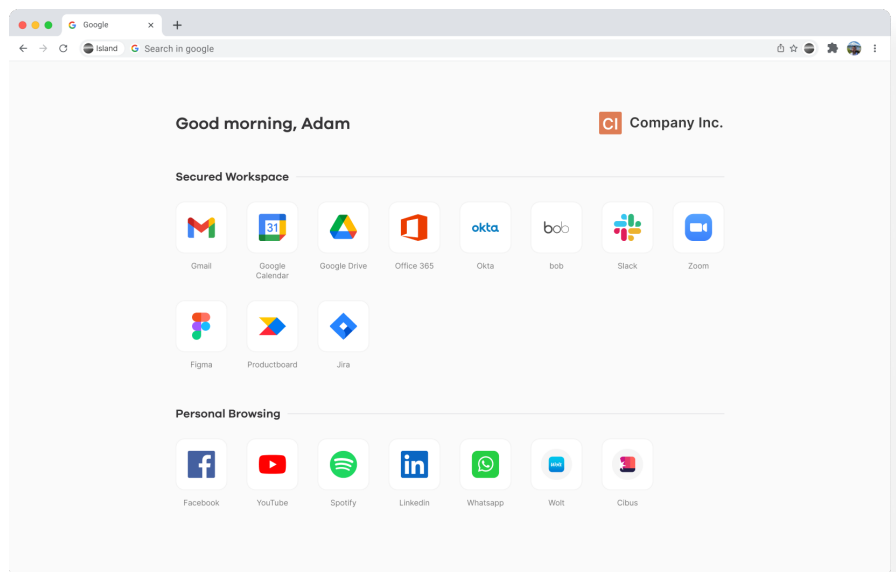
Quote from a Citrix end-user posted on G2.com
<https://www.g2.com/products/citrix-citrix-daas/reviews/citrix-daas-review-177668>

User feedback like this is very common with real-world DaaS or VDI deployments. Don't mistake this for a complaint about unreasonable users; it's quite the opposite. In 2022, your employees can and should expect a fast, efficient platform that enables productivity and doesn't get in the way.

The Enterprise Browser

The benefits of the SaaS software model for both software vendors and their customers is beyond dispute. The proliferation of cloud-scale technologies and Infrastructure-as-a-Service makes it possible to deliver in-house apps in a similar fashion. Modern app developers often choose progressive web apps rather than thick apps for optimal cross-platform deployments. For example, both Slack and Zoom are progressive web apps, and their desktop apps are actually a single-purpose browser. When all your mission-critical apps and data are flowing through the web, it makes a lot of sense to choose a web browser that's built for the enterprise. Here's how The Enterprise Browser can secure SaaS or web-app access, without any of the costs or complexity of a virtualized desktop:

- The Enterprise Browser can be configured as the only access point for SaaS & in-house web apps
- Users authenticate with your corporate identity provider in order to access the browser, so you can establish trust for every web app visit
- The Enterprise Browser launches with a home page you configure with links to common apps
- You define granular security controls that are context-aware of the user, device, network, and application



- The Enterprise Browser protects sensitive data with last-mile controls to govern printing, copy/paste, screen captures, upload/download
- Data security and user productivity are balanced with secure file storage that allows for transferring sensitive data between business apps, without that data ever reaching the local desktop
- The Enterprise Browser protects against malware, phishing attacks, man-in-the-middle attacks, and other browser exploits
- You can collect forensic audit logs over all browser activity with granular control over the depth of what is captured by user, device, application and location
- The Enterprise Browser is built on Chromium with a look and feel that's instantly familiar and a user experience that's fast and lightweight



Customer Example: Retail POS

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.

Remote Workers

All the advantages of The Enterprise Browser for secure web app access apply to a worker in the corporate office, a home office, or connecting remotely while traveling. Remote workers are more likely to face network interruptions so they're particularly sensitive to user experience issues with desktop virtualization. A traveling employee who connects on low-bandwidth airplane or hotel connections will especially benefit from The Enterprise Browser.

All the advantages of The Enterprise Browser for secure web app access apply to a worker in the corporate office, a home office, or connecting remotely while traveling.

For employees that need occasional remote access, The Enterprise Browser is an ideal solution for connecting from a personal computer. A user can download and install the browser without IT support and authenticate with their corporate identity. Now they have a secure portal to access company resources, with full isolation between their personal and business content. Since The Enterprise Browser is fully aware of the device it's running on, you can define the appropriate policies and security controls for a personal PC that's different from a company-issued laptop.

Contractor Access

Many operations rely on contractors or third parties to fill critical roles. For some businesses, a third-party organization takes on an entire function like logistics management or HR. Others use contractors to staff-up teams for project work. Regardless of the role they play, security controls are essential to protect the sensitive information they have access to. The nature of contract work means frequent turnover, so onboarding efficiency is especially critical. Some organizations choose to configure and ship a new laptop to each contractor. Others choose to offer a virtual desktop that the contractor installs on their computer. Either path resolves the security and access issue, but increases the cost to your organization.

Enterprise Browser doesn't require administrator privileges to run, and only takes a minute to install. On the first launch, they're prompted to authenticate with your enterprise identity provider

The Enterprise Browser offers a path for efficient contractor onboarding: contractors use their own computer to download the Island installer. The Enterprise Browser doesn't require administrator privileges to run, and only takes a minute to install. On the first launch, they're prompted to authenticate with your enterprise identity provider. The credentials you assigned carry the privileges aligned with their role, and in seconds they begin working. As mentioned above, you can configure The Enterprise Browser as the only entry point for your SaaS and in-house web apps, and add last-mile controls to stop data leakage. Especially crucial for contractor access is visibility: you can collect deep forensic audit logging and output events to data aggregation environments such as SIEM. When the contract is over and you revoke their credentials, The Enterprise Browser terminates any open browsing sessions and returns to the login page. No company data is left behind.



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.

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.

It's at this moment that organizations are rethinking their use of desktop virtualization in the name of efficiency and user experience

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.

